SAVONIA

OPINNÄYTETYÖ - **YLEMPI AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

DIGITAALISEN TURVALLI-SUUDEN JOHTAMINEN

Yara Suomi Oy, Siilinjärven toimipaikka

TEKIJÄ: Joel Kanniainen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Teknologiaosaamisen johtamisen tutkinto-ohjelma	
Työn tekijä Joel Kanniainen	
Työn nimi Digitaalisen turvallisuuden johtaminen Yara Siilinjärven toimipaikalla	
Päiväys 26.3.2020	Sivumäärä/Liitteet 50/1
Ohjaaja(t) Lehtori Pasi Lepistö, Tutkimuspäällikkö Jenni Toivanen	
Toimeksiantaja/Yhteistyökumppani(t) Yara Suomi Oy / HESQ-päällikkö Jukka Taskinen	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli selvittää Yara Siilinjärven toimipaikan digitaalisen turvallisuuden nykytilaa ja etsiä kehityskohteita, joita parantamalla digitaalisen turvallisuuden tasoa voidaan nostaa. Työn keskeisenä tavoitteena on avata digitaalisen turvallisuuden sisältöä henkilöille, jotka eivät työskentele sen edistämisessä päivittäin, vaan ovat lähtökohtaisesti loppukäyttäjiä.

Opinnäytetyössä perehdyttiin digitalisaation mukanaan tuomiin haasteisiin ja esitellään näiden vaikutuksia yrityksen toimintaan. Keskeisenä osana digitaalisen turvallisuuden johtamisessa on Yaran jatkuvan parantamisen toimintamalli. Digitaalisen turvallisuuden hallinnan perusteena on riskien arviointi. Työssä käytiin läpi digitaaliseen turvallisuuteen soveltuvia riskien arviointimenetelmiä ja periaatteita.

Työssä perehdyttiin lainsäädäntöön ja asetuksiin, jotka vaikuttavat digitaalisen turvallisuuden johtamiseen. Opinnäytetyössä käsiteltiin organisaation digitaalisen turvallisuuden prosesseja. Prosessit täytyi ymmärtää, jotta tietoturvan sisällään pitämät neljä kokonaisuutta: kyberturvallisuus, digitaalinen turvallisuus, tietoturvallisuus sekä tietotekninen turvallisuus saatiin avattua ja ymmärrettiin niiden yhteydet ja eroavaisuudet. Työssä avattiin eri organisaatiotasojen vastuita ja tehtiin digitaalisen turvallisuuden hallintamalli vuosikelloon perustuen.

Opinnäytetyön lopputuloksena saatiin tietopaketti, jonka avulla toimipaikan henkilöstön tietoisuutta digitaalisesta turvallisuudesta voidaan lisätä.

Avainsanat
digitaalinen turvallisuus, jatkuva parantaminen, johtaminen, kyberturvallisuus, gdpr, digitalisaatio

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Master's Degree Programme in Engineering Knowledge Management			
Author Joel Kanniainen			
Title of Thesis Digital Security Management at Yara Siilinjärvi Site			
Date	26 March 2020	Pages/Appendices	50/1
Supervisor(s) Senior lecturer Mr. Pasi Lepistö, Research Manager Mrs. Jenni Toivanen			
Client Organisation /Partners Yara Suomi Oy/ HESQ Manager Mr. Jukka Taskinen			

Abstract

The aim of this thesis was to clarify the current state of digital security at the Yara Siilinjärvi site and to find some development areas in digital security. The key aim of this thesis was to introduce digital security for those who are not digital security specialists and who do not work with that daily. Based on the identified development areas, measures were identified to increase the level of digital security at the site.

The thesis views the challenges of digitalization and presents their impacts on the company's operations. The digital security management is based on risk assessments and it is made by the Yara's continuous improvement model. The suitable risk assessment models and processes for digital security were studied in this thesis.

The legislations and the regulations that affect digital security management as well as digital security were studied. The thesis dealt with the digital security processes of the organization. Digital security includes several terms (for example cyber security, information security) that were specified in the thesis. The thesis studied digital security management responsibilities at different organizational levels and presents a management model based on an annual clock.

As a result of this thesis, an information pack was drawn up that will benefit the readers i.e. the end users of this pack so that the level of digital security among the staff can be increased.

Keywords
digital security, continuous improvement, management, cyber security, gdpr, digitalization

ESIPUHE

Toimin päivittäisessä työssäni Security Engineer nimikkeellä Yara Suomi Oy:ssä ja olen etuoikeutettu olemaan mukana turvaamassa henkilöstöä, tuotantoa ja omaisuuttamme. Digitaalisuus on mahdollistanut paljon, mutta se on tuonut mukanaan uusia haasteita sen hallintaan ja johtamiseen liittyen.

Omassa tehtävässäni merkittävässä roolissa on herätellä henkilöstöämme ja yhteistyökumppaneitamme valppauteen tietoturvallisessa toiminnassa sekä lisätä heidän tietoisuuttaan mitä riskejä digitaalisuus tuo mukanaan.

Yara tunnetaan työelämässä korkeasta turvallisuustasostaan, jonka ihmiset pääsääntöisesti mieltävät työturvallisuuteen liittyviin turvallisuusasioihin. Turvallisuus sanana on suomenkielessä haastava, koska se pitää sisällään kaiken; niin työ-, prosessi-, henkilö-, toimitila-, alue-, yritys- kuin digitaalisen turvallisuudenkin. Jotta voimme tulevaisuudessakin pysyä kilpailukykyisinä tulee meidän olla aallonharjalla tai olla ainakin nousemassa kovaa vauhtia sinne kaikilla turvallisuuden sektoreilla.

Haluan kiittää Yaraa mahdollisuudesta täydentää omaa tiedonjanoani opiskelemalla työni ohessa. Erityisesti haluan kiittää esimiestäni Jukka Taskista, joka on luottanut osaamiseeni ja antanut mahdollisuuden toteuttaa omia visioitani kohti (digitaalisestikin) turvallisempaan Yaraa.

Kuopiossa 26.3.2020
Joel Kanniainen

SISÄLTÖ

Lyhenteet ja määritelmät

HOPS	HESQ Operating Standard
ICT	Information and Communications Technology. Tieto- ja viestintäteknologia
IDS	Intrusion Detection System, Tunkeilijan havaitsemisjärjestelmä
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.
IT	Information Technology, tietotekniikka
Loppukäyttäjä	Henkilö joka loppukädessä käyttää tuotetta tai palvelua
MFA	Multi-factor authentication, monivaiheinen tunnistautuminen
PDCA	Plan, Do, Check, Act. Suunnittele, tee, tarkista, korjaa ongelmien ratkaisumalli.
SSPR	Self Service Password Reset, salasanan itse nollaaminen
VPN	Virtual Private Network, virtuaalinen erillisverkko
Yara	Yara International ASA, Yaran pääyhtiö
Yara Suomi Oy	Yara Suomi Oy, Yaran Suomen maayhtiö
YMS	Yara Management System, Yaran johtamisjärjestelmä

1 JOHDANTO

Teollisuuden ja sen toimintaympäristöjen muutos digitaalisuuteen on ollut muutaman vuoden aikana voimistuva trendi. Rikollisuus on entistä enemmän siirtynyt fyysisistä toimista verkkoon ja kidnappaukset ovat muuttunut henkilöistä suurteollisuuden ohjelmistojen ja järjestelmien kaappaamiseen. Turvallisuutta ei voida kokonaisuudessaan johtaa enää vartioiden ja pelkkien fyysisten aitalinjojen avulla. Sosiaalinen media toimii voimakkaana informaatiovaikuttamisen alustana ja se tavoittaa hetkessä laajoja joukkoja, joiden mielenkiinto tai tavoite on yhteinen.

Päivittäinen työ on siirtynyt entistä enemmän verkossa tehtäväksi, työmatkustaminen on vaihtunut Skype ja Teams videoneuvottelukokouksiin ja data eli meidän arvokas tietopääomamme on tallennettuna USB-tikkujen ja kovalevyjen sijasta pilvipalveluihin, josta tätä dataa on mahdollista käyttää millä tahansa älylaitteella.

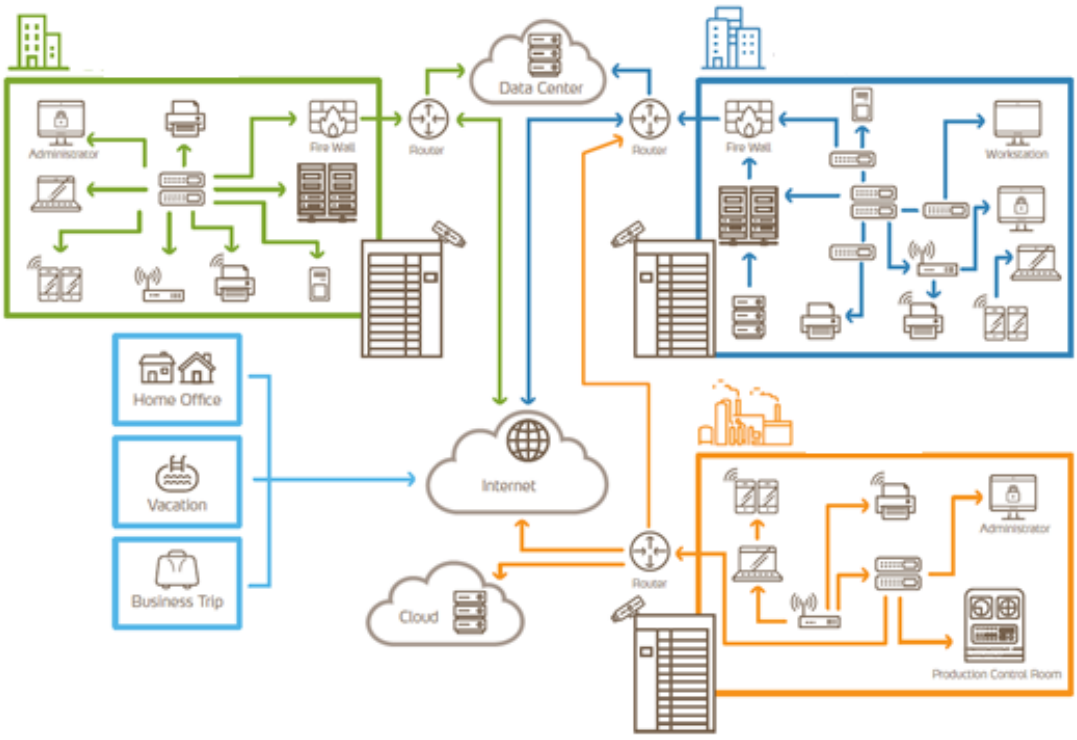
Pilvipalvelut ja muut digitalisoituneet työskentelyalustat tarjoavat aivan uusia mahdollisuuksia etätyöhön ja viimeisin data on aina käytettävissä – ilman VPN yhteyksiä tai muita kirjautumistapoja yrityksen omaan verkkoon. Pilvipalveluissa säilytettävä data on hajautettuna palveluntarjoajien palvelinsaleihin ympäri maailmaa. Näitä palvelinsaleja uhkaavat vesivahingot, tulipalot, sabotaasi ja muut mahdolliset mullistukset voidaan lähtökohtaisesti hallita teknisillä ratkaisuilla pitkälle ja tällöin meille heikoimmaksi turvallisuuden lenkiksi jää palvelun loppukäyttäjä.

Palvelualustojen digitalisaatio on tuonut paljon vapauksia, mutta harva käyttäjä tiedostaa vastuita, joita nämä digitalisoitumiset ovat tuoneet mukanaan. Loppukäyttäjälle jää suuri vastuu toimia oikein digitaalisessa pelikentässä. Käyttäjätunnus ja salasana yhdessä ovat voimakkain ja helpoin tapa päästä käsiksi kaikkeen yrityksen tietopääomaan, mistä päin maailmaa tahansa.

Digitaaliseen turvallisuuteen liittyvät vaarat ja riskitekijät näyttäytyvät loppukäyttäjälle useimmiten harmittomilta näyttäviltä asioilta työpöydällä tai elementteinä sähköpostien mainosbannereissa. Loppukäyttäjä voi tahallisesti tai useimmiten tahattomasti tehdä toiminnallaan valtavan suuren rahallisen tappion työnantajalleen.

Kahvihuoneen pöydältä löydetty usb-tikku saa valitettavan usein loppukäyttäjän uteliaisuuden heräämään ja saa henkilön toimivaan vastoin annettuja turvallisuusohjeita ja työntämään tallennusmedian kiinni omaan tietokoneeseensa. Käyttäjä yleensä havaitsee virheensä vasta, kun vahinko on jo päässyt tapahtumaan ja olemme tilanteessa, jossa koko yritysverkon laitteisto ja data on saastunut.

Alla oleva havainnekuva (KUVA 1) antaa hyvää perustietoa siitä, missä kaikkialla nykyään digitaalisuus näkyy ja mihin kaikkeen rikollisilla voi olla pääsy, jos he saavat loppukäyttäjän käyttäjätunnuksen ja salasanan haltuunsa.



Kuva 1. Kuvassa on esimerkki verkottuneesta teollisuusympäristöstä. (YARA, Yara Security Management, International ASA, 2019a).

1.1 Tavoitteen määrittely

Opinnäytetyön tavoitteena on perehtyä Yara Siilinjärven toimipaikan digitaalisen turvallisuuden nykytilaan ja selvittää millä toimenpiteillä digitaalista turvallisuutta voidaan toimipaikalla kehittää. Nykytilavertailu tullaan tekemään vertailuna DNV:n itsearviointimateriaaliin perustuen. Opinnäytetyön tulee olla tietopaketti henkilöstölle, jonka avulla henkilöstön tietoisuutta digitaalisesta turvallisuudesta voidaan kasvattaa. Työssä avataan lainsäädäntöä ja asetuksia, jotka vaikuttavat digitaalisen turvallisuuden hallintaan.

Työssä on tarkoitus syventyä digitaaliseen turvallisuuteen ja avata henkilöstölle mitä osa-alueita tämä pitää sisällään. Uutisissa, sosiaalisessa mediassa ja yrityksien materiaaleissa näkyy muun muassa termejä: Tietoturvallisuus, tietotekninen turvallisuus, digitaalinen turvallisuus, kyberturvallisuus, tietoturvataso sekä GDPR, mitä eroa ja yhteistä näillä on ja kuinka nämä liittyvät toisiinsa? Tämän opinnäytetyön luettuaan lukijalla tulee olemaan peruskäyttäjää syvempi osaaminen ja termistö hallussa.

Yara noudattaa toiminnassaan jatkuvan parantamisen periaatteita ja työssä läpikäydään digitaalisen turvallisuuden hallintaa jatkuvan parantamisen periaatteiden mukaisesti.

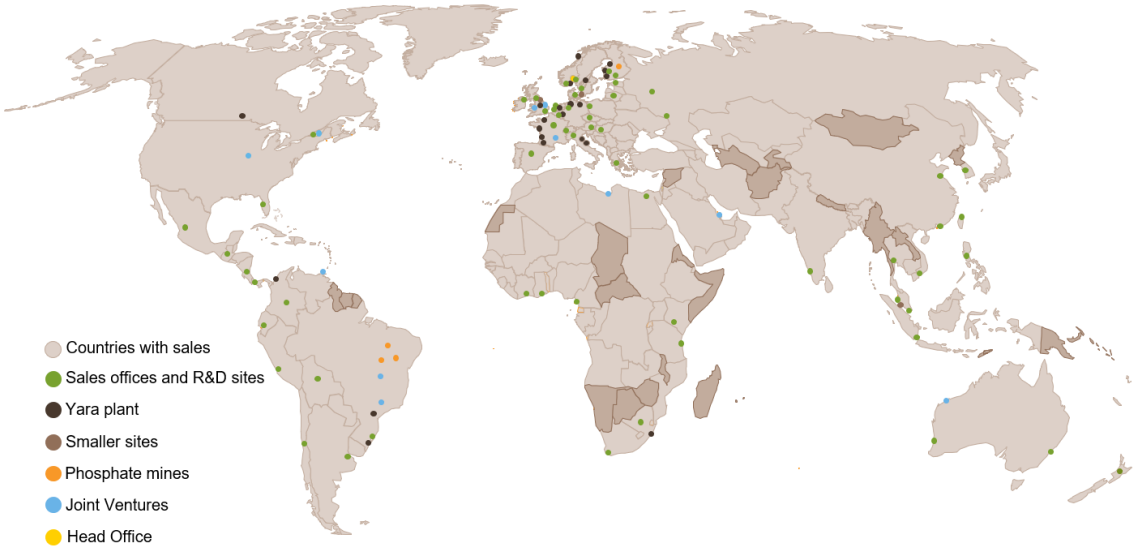
1.2 Yara Suomi Oy esittely

Yara on maailmanlaajuinen kivennäislannoitteiden, teollisuuskemikaalien ja ympäristönsuojelutuotteiden toimittaja. Yaralla on 16 000 työntekijää noin 60 massa. Toimintaamme kuuluu yli 20 tuotantolaitosta ja 3 tutkimuskeskusta. Yrityksen liikevaihto oli vuonna 2018 noin 10 miljardia euroa. Maailmanlaajuisesti Yaran tuotteiden avulla tuotetaan 240 miljoona tonnia viljaa, ruokitaan 240 miljoonaa ihmistä ja puhdistetaan ilmaa 50 miljoonalle ihmiselle. Yrityksen missiona on maailman väestön ruokkiminen vastuullisesti ja planeettamme suojeleminen, visiona on yhteiskunta, jossa tehdään yhteistyötä; maailma ilman nälänhätää; planeetta, jota kunnioitetaan (KUVA 2). Yaran päivittäisessä toiminnassa näkyvät arvot ovat uteliaisuus, kunnianhimo, yhteistyö ja vastuunotto.

Yaralla on Suomessa kolme tuotantolaitosta: Siilinjärvellä, Uudessakaupungissa ja Kokkolassa. Siilinjärvellä on lisäksi Länsi-Euroopan ainoa toimiva fosfaattikaivos. Kotkaniemen koetilalla on ollut t & k toimintaa yli 50 vuoden ajan. Yara Suomen maakonttori sijaitsee Espoossa. Suomessa tuotetaan 1,5 miljoona tonnia lannoitteita, josta ¾ menee vientiin ja teollisuustuotteita 160 000 tonnia, joista ¼ menee vientiin. Suomessa Yara työllistää suoraan 900 henkeä ja työllisyysvaikutus on yhteensä noin 4000 henkilötyövuotta. Yara on investoinut Suomeen 2008 – 2019 noin 900 miljoonaa euroa, joista pelkästään Siilinjärvelle 600 miljoonaa euroa.

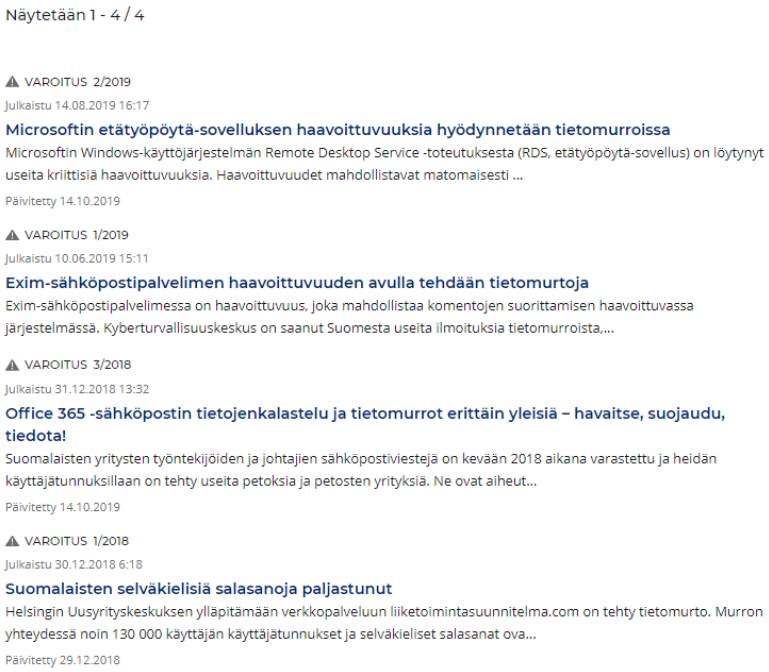
Yaran turvallisuusperiaatteena on, että tunnistamme ja hallitsemme toimintaamme liittyvät riskit. Lähtökohtanamme on, että kaikki vahingot ovat estettävissä. Teemme joka hetki valintoja, joilla otamme vastuun turvallisuudesta ja sen kehittämisestä niin omassa työssämme kuin kaikessa toimipaikkamme toiminnassa. Yara Siilinjärven tehtaille on myönnetty ISO 45001 Työterveyden- ja työturvallisuuden johtamissertifikaatti. (YARA, Esittelymateriaali, Yara Suomi Oy, 2020.)

Kuva 2. Kuvassa on esiteltynä Yaran Missio, Visio ja Arvot. (YARA, Esittelymateriaali, Yara Suomi Oy, 2020).



Kuva 3. Yaran toimipisteiden sijainnit kartalla. (YARA, Esittelymateriaali, Yara Suomi Oy, 2020).

Yaran toiminta maailmanlaajuisesti (KUVA 3) asettaa eri toimipaikat alttiiksi hyvin erityyppisille digitaalisen turvallisuuden vaaroille. Yara Suomi Oy, Siilinjärven tehtaat sijaitsevat kyberturvallisuuden kannalta toistaiseksi melko rauhallisella alueella. Suomessa toimintaan ei myöskään kohdistu sotatoimia, jotka aiheuttaisivat merkittävää vaaraa security -turvallisuusosa-alueen kannalta. Suomessa kyberturvallisuuskeskus seuraa toimintaa aktiivisesti ja tekee varoituksia mahdollisista riskeistä. Kyberturvallisuuskeskuksen sivuilta löytyvien varoitusten määrästä (neljä) (KUVA 4) voidaan päätellä, että toistaiseksi Suomessa olemme turvallisemmassa asemassa, kuin monessa muussa toimipaikassamme.


Näytetään 1 - 4 / 4

⚠ VAROITUS 2/2019
Julkaistu 14.08.2019 16:17
Microsoftin etätyöpöytä-sovelluksen haavoittuvuuksia hyödynnetään tietomurroissa
Microsoftin Windows-käyttöjärjestelmän Remote Desktop Service -toteutuksesta (RDS, etätyöpöytä-sovellus) on löytynyt useita kriittisiä haavoittuvuuksia. Haavoittuvuudet mahdollistavat matomaisesti ...
Päivitetty 14.10.2019

⚠ VAROITUS 1/2019
Julkaistu 10.06.2019 15:11
Exim-sähköpostipalvelimen haavoittuvuuden avulla tehdään tietomurtoja
Exim-sähköpostipalvelimessa on haavoittuvuus, joka mahdollistaa komentojen suorittamisen haavoittuvassa järjestelmässä. Kyberturvallisuuskeskus on saanut Suomesta useita ilmoituksia tietomurroista,...

⚠ VAROITUS 3/2018
Julkaistu 31.12.2018 13:32
Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota!
Suomalaisten yritysten työntekijöiden ja johtajien sähköpostiviestejä on kevään 2018 aikana varastettu ja heidän käyttäjätunnuksillaan on tehty useita petoksia ja petosten yrityksiä. Ne ovat aiheut...
Päivitetty 14.10.2019

⚠ VAROITUS 1/2018
Julkaistu 30.12.2018 6:18
Suomalaisten selväkielisiä salasanoja paljastunut
Helsingin Uusyrityskeskuksen ylläpitämään verkkopalveluun liiketoimintasuunnitelma.com on tehty tietomurto. Murron yhteydessä noin 130 000 käyttäjän käyttäjätunnukset ja selväkieliset salasanat ova...
Päivitetty 29.12.2018

Kuva 4. Kyberturvallisuuskeskuksen voimassa olevat varoitukset. (TRAFICOM, Kyberturvallisuuskeskus - Varoitukset, 2020).

1.3 Miksi digitaalinen turvallisuus on tärkeää ja millaisia riskejä siihen liittyy?

Digitaalisessa turvallisuudessa on tärkeää tunnistaa merkittävimmät järjestelmät ja aloittaa suojaustoimenpiteet näistä ”kruunun jalokivistä”. Kaikki kriittiset järjestelmät ovat suunniteltu jotain tiettyä toimintoa varten. Mikäli tämä toiminallisuus katoaa järjestelmään kohdistuneen hyökkäyksen takia, voi sillä olla merkittäviä vaikutuksia tuotantoon, turvallisuuteen tai ympäristöön. Mikäli nämä kriittiset järjestelmät on tunnistettu tehokkaasti ja niiden toiminta on asianmukaisesti suojattu, on tällä merkittävä vaikutus digitaalisen turvallisuuden tason paranemiseen. (BYRES, 2013.)

Johdannossa todettiin jo, kuinka teollisuus on digitalisoitunut ja pilvipalvelut ovat jo arkipäivää ainakin suurempien yritysten toiminnassa. Viimeksi digitaalisessa toiminnassa on koettu vastaavia kehitysaskeleita, kun mobiiliverkot muuttivat toimintamallia pari vuosikymmentä sitten. Pilvipalvelut ovat jokaisella osa arkea ja pidämme niitä täysin itsestään selvinä. Loppukäyttäjä pysähtyykin ajattelemaan pilvipalvelua ja sen toimintaa monesti vasta kun se ei enää toimi. Pilvipalvelut toimivat suurissa datakeskuksissa, josta ne hiljalleen hajautuvat osaksi meidän kaikkien elämäämme.

Partnerin arvio on, että maailmassa on vuonna 2021 jo yli 25 miljardia verkkoon liitettyä laitetta. Nämä laitteet muodostavat meidän jokapäiväisessä käytössämme olevista laitteista, kuten älykelloista, matkapuhelimista, kannettavista tietokoneista sekä palvelimista – yhdessä kaikki nämä laitteet muodostavat hajautetun, kaikkialla saatavissa olevan laskentakapasiteetin. Teknologian kehittyessä sekä tekoälyn lisääntyessä tarvitsemme entistä enemmän laskentatehoa, mahdollisimman lähellä loppukäyttäjää, jotta toiminnallisuuksia saadaan lisää käyttäjien laitteisiin. Mitä enemmän mahdollisuuksia laitteisiimme tulee, sitä kysytympää laskentateho on ja se altistaa meidät lisääntyville riskeille. (VIITAILA, 2019.)

Millaisia vaikutuksia digitaalisen turvallisuuden laiminlyönnillä voi olla yritykselle? Mikäli digitaaliseen turvallisuuteen kohdistuva hyökkäys vahingoittaisi merkittävästi yrityksen mainetta, sen osakekurssi voisi kokea merkittävää laskua. Yrityksen liikevaihto putoaisi, mikä voisi johtaa yrityksen syöksykierteeseen ja lopulta johtaa konkurssiin. Paras tapa estää tämä, on pysäyttää se jo ennen kuin se on alkanut. Toimitusjohtajien on ymmärrettävä, että heidän tulee sijoittaa entistä enemmän tälle strategiselle osa-alueelle, digitaalisen turvallisuuden hallintaa ei voi sysätä vain teknisille asiantuntijoille. (D'antonio, 2019.)

Traficom Liikenne- ja viestintäviraston kyberturvallisuuskeskus ylläpitää ja julkaisee kuukausittain Kybersään (KUVA 5). Kybersää kertoo helposti koostettuun muotoon edellisen kuukauden merkittävät tietoturvapoikkeamat- ja ilmiöt. Sää on pääsääntöisesti tietoturvallisuuden asiantuntijoille suunnattu lukupaketti. Kybersäästä saa nopeasti yleiskuvan kyberturvallisuuskentän tapahtumista julkaisukauden aikana. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020.)

Kuva 5. Kuvakaappaus kyberturvallisuuskeskuksen Kybersäästä, Tammikuu 2020. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020).

1.3.1 Löydettyjen haavoittuvuuksien nopea hyödyntäminen

Tietoturva-aukkojen ja haavoittuvuuksien hyödyntäminen on nopeutunut, mikä edellyttää entistä nopeampia korjauspäivityksiä. Tietoturvaa ei huomioida riittävällä tasolla, kun verkossa olevia laitteita hallinnoidaan. Verkkoon jääkin auki laitteita, joiden tietoturvan suojaustoimet sekä ylläpito ovat puutteellisia. Tietoturvarikolliset kehittävät nopeasti hyväksikäyttömenetelmiä heti mahdollisten ohjelmistopäivitysten ilmestyttyä. Heidän toimintamallina on iskeä kohteisiin, joita ei ole päivitetty. Tietoturvatuotteiden puutteet ovat erityisen vakavia, koska ne on monesti sijoitettu jo valmiiksi hyökkäyksille alttiisiin järjestelmiin.

Järjestelmähaavoittuvuudet, joita on käytetty hyökkäyksissä ovat usean olleet noin 2 – 6 kk vanhoja haavoittuvuuksia. Näihin tietoturvahaavoittuvuuksiin on ollut saatavilla korjauspäivitys jo pidemmän aikaa, mutta jostain syystä haavoittuvuutta ei ole korjattu. Mitä kauemmin korjauspäivityksen asentamista viivytellään, sitä korkeammaksi kasvaa hyväksikäyttämisen riski. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020.)

1.3.2 Tietojenkalastelun merkittävä kasvu

Tietojenkalastelu (phishing) on yksi yleisimpiä menetelmiä tietoturvarikollisten keskuudessa. Tietojenkalastelussa käyttäjän voi monesti olla hankala tunnistaa huijausta. Tietokojenkalasteluissa käytettävät viestit ovat usein erittäin aidonnäköisiä ja muotoiltu siten, että ne eivät herätä loppukäyttäjässä epäilyksen tunnetta. Tietojenkalastelua voidaan hyödyntää hyvinkin kohdennetuissa hyökkäyksissä tai vakoiluyrityksissä. Kalastelu voidaan kohdentaa esimerkiksi organisaation HR-henkilöstöön tai johdon käyttäjätileihin.

Pitkän aikavälin tarkastelussa tietojenkalastelu on ollut erittäin yleistä. Yritykset ovat siirtyneet entistä enemmän pilvipohjaisiin ratkaisuihin ja tästä johtuen yleisin toimintamalli on kalastella suomalaisten käyttäjätunnuksia ja salasananoja Office 365 -tuotteisiin ja sähköpostiin. Mikä rikollinen saa haltuunsa käyttäjän Officen tunnukset, hänellä on helppo pääsy kaikkiin pilvipalvelun tuotteisiin kuten One Drive tallennuksiin, sähköpostiin ja One Note muistiinpanoihin.

Ilmiöön yhdistetään vahvasti myös typosquatting / domainsquatting eli muokataan verkkotunnuksia tai sähköpostiosoitteita pienillä kirjoitusvirheillä, joilla voidaan tehostaa huijauksen vaikuttavuutta organisaatiossa. Yksi käytetyimpiä esimerkkejä on muuttaa O-kirjain 0-numeroksi. Esimerkiksi esimerkki@O365.com vs. esimerkki@0365.com. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020.)

1.3.3 Laajavaikutteinen kiristyshyökkäys

Liiketoiminnan jatkuvuutta pyritään uhkaamaan laajavaikutteisilla kiristyshyökkäyksillä (Big Game Hunting). Merkittävimmissä yksittäistapauksissa vahingot ovat voineet nousta jopa kymmeniin miljoonin euroihin. Suomessa on myös tapauksia, suurin osa näistä organisaatioista valikoituvat kohteeksi sattumalta. Verkoista etsitään jatkuvasti haavoittuvia palveluita ja heikkoja salasanoja. Mikäli kyberrikolliset havaitset arvokkaan, huonosti suojatun verkkoympäristön, siihen voidaan mahdollisesti kohdentaa Big Game Hunting -toimintaa. Yhdysvalloissa laajavaikutteisten kiristyshyökkäysten tilannetta voidaan kuvata jo epidemiaksi. Laajoista kiristyshaittaohjelmatartunnoista saadaan kansainvälisesti viestiä ja ilmoituksia viikoittain.

Teollisuus on saanut kiristyshyökkäyksistä oman osansa. Norjassa Norsk Hydroon kohdistettiin kiristyshaittaohjelma, joka levisi tuotantojärjestelmiin asti. Yrityksen toiminnassa oli häiriöitä useita kuukausia ja hyökkäys kosketti useita yrityksen toimipaikkoja. Vahingon suuruudeksi Norsk Hydro arvioi omilla verkkosivuillaan noin kuusikymmentä miljoona euroa. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020.)

1.3.4 Epäselvät vastuut yrityksen tietoturvassa

Tietoturvan hallinta ei ole vahvaa, mikäli vastuunjako palvelutoimittajan, alihankkijoiden sekä tilaajan välillä on epäselvää. Mikäli lokeja ei tarkkailla tämä vaikeuttaa tietoturvauhkien havaitsemista ja niihin reagoimista. Vastuiden epäselvä jako koskee myös oman organisaation toimintaa. Mikäli tietoturvariskien tietoturvavastuut ja omistajuudet eivät ole selkeästi määriteltyjä, vaikuttaa se negatiivisesti yrityksen tietoturvatasoon. Mikä vastuunjako jää epäselväksi on yleinen puute jättää keräämättä ja tarkastelematta tietoturvalokeja.

Usein tietoturvaloukkaukset ja järjestelmien heikkoudet saadaan selville jatkuvalla tietoturvalokien tarkkailulla ja näin voidaan saattaa puutteet kuntoon, ennen kuin kukaan ehtii hyödyntää niitä suurempaan vahingontekoon. Lokeilla on suuri merkitys myös jälkikäteen tehtäessä selvityksiä tietoturvaloukkauksista. Muutoksen hallinta korostuu myös tietoturvan hallinnassa. Mikäli käytöstä poistetaan järjestelmiä tai ohjelmistoja, tulee muutoksen hallinnassa varmistaa se, että järjestelmät poistuvat käytöstä kokonaan. Mikäli vanhoja häntiä jää roikkumana, niitä ei enää päivitetä ja ne aiheuttavat merkittävän tietoturvaheikkouden. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020.)

1.3.5 Organisaatioiden osaamattomuus

Vakava puute digitaalisessa turvallisuudessa on organisaatioiden osaamattomuus hallita digitaalisia riskejään. Organisaatiot eivät aina osaa arvioida uhkien vaikutusta toimintaansa ja tästä johtuen eivät pysty ennakoida niitä, mikä johtaa riskien aliarviointiin. Palautumista tietoturvaloukkauksista ei usein suunnitelma huolellisesti ennakkoon, vaan suunnitelmat ovat luokkaa ”palautetaan tiedot varmuuskopioista”. Palautuminen tietoturvaloukkauksesta edellyttää normaalia suurempaa resursointia ja mikäli toimintamalleja ei ole määritelty palautumissuunnitelmassa se hidastaa palautusprosessien käynnistämistä.

Palautuminen häiriöstä osoittautuu usein monimutkaiseksi ja työlääksi, mikä tulee organisaatiolle yllätyksenä, mikäli palauttamiseen ei ole valmistauduttu. Mikäli toimintaa olisi suunniteltu ennakkoon paremmin, myös varautuminen häiriöihin sekä niiden ehkäisemiseen ennalta olisi parempaa. Yrityksen ylimmän johdon tulee varmistua oman organisaationsa kyvykkyydestä arvioida tietoturvariskejä ja tehdä toimenpiteitä, jotta varmistutaan henkilöiden kouluttamisesta jatkuvan parantamisen periaatteiden mukaisesti. (TRAFICOM, Kyberturvallisuuskeskus - Kybersaa, 2020.)

2 TEORIAPERUSTA JA LAINSÄÄDÄNTÖÄ

Tietoturva tarkoittaa Yaran tietojen ja omaisuuden suojaamista. Tavoitteena on varmistaa, että tiedot ja järjestelmät ovat: virheettömiä, käytettävissä tarvittaessa ja ainoastaan valtuutettujen henkilöiden käytettävissä tarpeen mukaan.

2.1 Digitaalisen turvallisuuden keskeiset velvoitteet ja tavoitteet

Digitaalinen turvallisuus ja tietosuoja koskevat käytännössä kaikkia Yaran työntekijöitä. Voit kysyä itseltäsi muutaman kysymyksen: Oletko vastuussa henkilöstöstä, oletko yhteydessä asiakkaisiin, alihankkijoihin tai toimittajiin? Oletko Yaran työntekijä? Olet todennäköisesti vastannut myöntävästi vähintään yhteen kysymykseen, joten tietosuoja koskee myös Sinua!

Henkilötietoja ovat esimerkiksi:

- Nimi, osoite ja puhelinnumero
- Henkilötunnus
- Henkilöiden kuvat
- IP-osoitteet
- Asiakkaille tarkoitetut yhteystietoja sisältävät käyntikortit

Mitkä ovat Sinun velvollisuutena tietosuojaan liittyen?

- Suorita tietosuojaa koskeva verkkokoulutus.
- Tutustu tietosuojaohjeisiin, toimintastandardeihin ja menettelytapoihin sekä Pulsen tietosuojaperiaatteisiin.
- Luokittelu ja merkitse henkilötietoja sisältävät tiedot.
- Suojaa (esim. salaa) aina asiakirjat ja sähköpostit asianmukaisesti (käytä Yaran tietojen suojaustyökalua).
- Tarkista sähköposti sekä henkilökohtaiset kansiot ja poista tarpeettomat tiedot.
- Ilmoita epäillyistä tai todellisista henkilötietojen loukkauksista.
- Jos sinulla on kysyttävää, ota yhteys tietoturvatiimiin osoitteessa.

Loppukäyttäjää koskevat tärkeimmät säännöt digitaaliseen turvallisuuteen liittyen:

- Suojaa aina tilisi ja salasanani, käytä eri palveluissa eri salasanoja.
- Säilytä Yara-tili luottamuksellisena. Se on kaikkien käytettävissä olevien tietojesi lähde.

Käytä:

- Self-Service Password Reset (SSPR) -toimintoa. Sen avulla voit vaihtaa salasanani tai poistaa tilisi lukituksen soittamatta Global Service Desk-tukipalveluun.
- Monivaiheista tunnistautumista (MFA - Multi Factor Authentication). Saat varoituksen, jos muut yrittävä käyttää tiliäsi.
- Noudata hyvää salasananhallintaakoskevia ohjeita.
- Salasanan tulee olla helposti muistettavissa, mutta muiden vaikeasti arvattavissa. (YARA, GDPR ohje, International ASA, 2019.)

2.2 EU tietosuoja-asetus

Tietosuoja-asetus eli yleisesti tunnetummin GDPR lainsäädäntö tulee sanoista General Data Protection Regulation (yleinen tietosuoja-asetus). Kyseessä on uusi laki, joka sääntelee henkilötietojen käsittelyä EU maissa. Lakia on sovellettu kaikissa EU-maissa 25.5.2018 alkaen.

Uusi lainsäädäntö on tehty parantamaan henkilötietojen suojaa ja tietosuojaoikeuksia. Lain tavoitteena on vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin. Laki mahdollistaa yhtenäisen tietosuojasääntelyn kaikissa EU-maissa. Tavoitteena on edistää digitaalisten sisämarkkinoiden kehittymistä. (TIETOSUOJA, GDPR, 2019.)

Uusi tietosuoja-asetus tuo henkilöille paljon oikeuksia, mutta henkilötietojen käsittelijöille entistä enemmän velvollisuuksia. Jokaisen yksilön on tärkeää tunnistaa omat oikeutensa, jotta voi valvoa oman oikeusturvansa toteutumista.

Tietosuoja-asetuksessa kerrotaan, ne oikeuden mitä käyttäjällä on, kun yritys tai organisaatio käsittelee henkilötietojasi. Käyttäjällä on oikeus:

- Saada tietoa omien henkilötietojen käsittelystä.
- Saada pääsy omiin tietoihin.
- Oikaista omia tietojaan.
- Poistaa omat tietonsa ja tulla unohdetuksi organisaatiossa tai yrityksessä.
- Rajoittaa omien tietojensa käsittelyä.
- Siirtää omat tiedot järjestelmästä toiseen.
- Vastustaa omien tietojen käsittelyä.
- Olla joutumatta automaattisen päätöksenteon kohteeksi

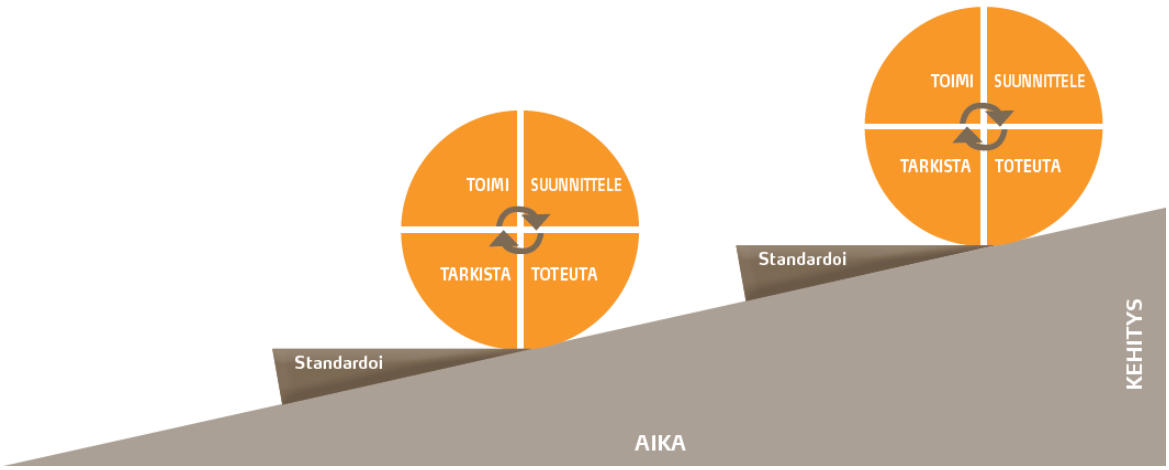
Käyttäjän tulee kuitenkin ymmärtää, että kaikkia oikeuksia ei voi soveltaa kaikissa tilanteissa. Oikeuksiaan soveltamiseen vaikuttaa muun muassa se, millä perusteella organisaatio tai yritys käsittelee henkilötietojasi. (TIETOSUOJA, Tunne oikeutesi, 2019.)

2.3 Tietoturvallisuuden hallintajärjestelmä – ISO 27001

Yritysten tietoturvaperiaatteiden hallinta ja niiden vertailu tulee olla yhdenmukaista ja läpinäkyvää toimintaan. ISO 27001 -sertifikaatti toimii todisteena, että organisaation tietoturvajohtamisjärjestelmä on sertifioitu parhaiden käytäntöjen mukaisesti ja että se täyttää kaikki standardin asettamat vaatimukset.

ISO 27001 -standardi tarjoaa prosessiperusteisen hyväksytyn tavan lähestyä organisaation tietoturvajohtamis- ja hallintajärjestelmän perustamiseen, toteuttamiseen, käyttämiseen, valvomiseen, päivittämiseen, huoltamiseen sekä parantamiseen.

Standardi on yhdenmukainen muiden johtamisjärjestelmien kanssa. ISO 27001 on harmonisoitu Yaralakin käytössä olevan ISO 14001 (ympäristöjohtaminen) ja ISO 9001 (laadunhallinta) kanssa. Standardi painottuu tietoturvajohtamisjärjestelmän prosessien jatkuvaan parantamiseen ja selkiyttämään rekistereihin sekä dokumentaatioihin liittyviä vaatimuksia. Riskien arvioinnin huomiointi ja prosessin ohjaus toteutetaan PDCA (Plan-Do-Check-Act) (KUVA 6) ongelmanratkaisumenetelmän avulla.



Kuva 6. Kuvassa on Yaran PDCA prosessi (YARA, International ASA, 2019).

ISO 27001 standardissa korostetaan tietoturvan merkitystä omaisuuden turvaamiseksi. Standardi antaa yritykselle käyttöön kattavan lähestymistavan tietoturva-asioihin. Suojattavia kohteita on muun muassa paperiasiakirjat, tietokoneet, digitaalinen tieto ja tietoverkot kokonaisuudessaan, pois jättämättä yksittäisten työntekijöiden tietotaitojakin. Standardissa esille nousevat seikat vaihtelevat henkilöstön pätevyydestä tekniseen suojaukseen tietokoneella tehtäviä väärinkäytöksiä vastaan. (DNV, 2020.)

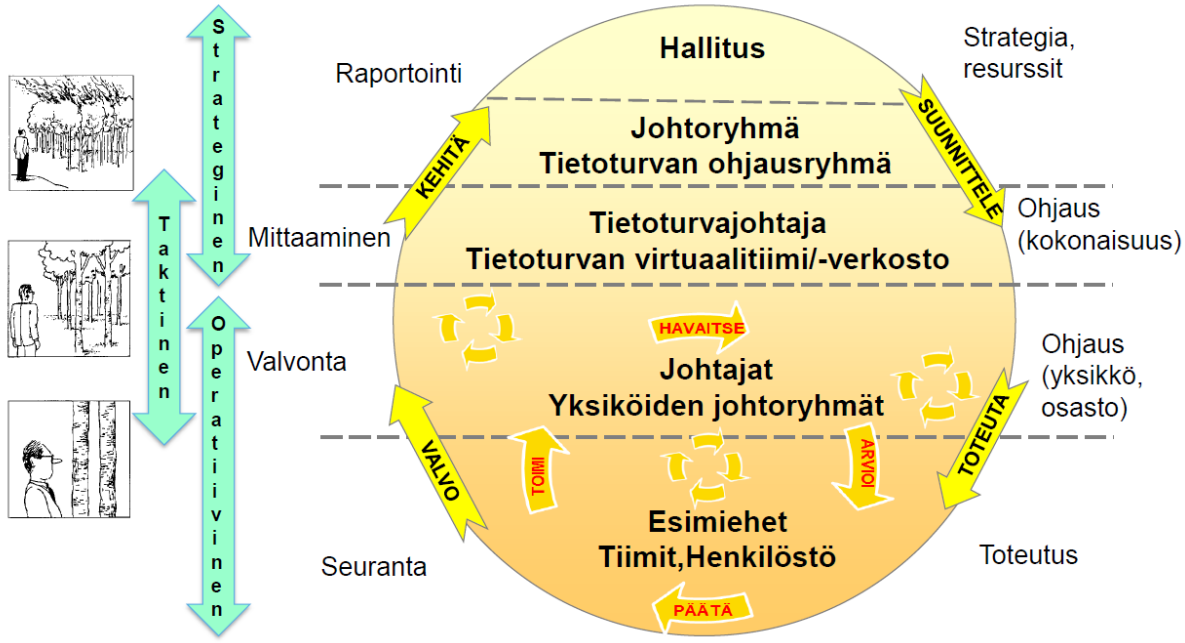
ISO 27001 standardin keskeisen sisältö avattuna kattaa seuraavien osa-alueiden tarkastelun

1. Tietoturvapolitiikat (2 hallintakeinoa)
    - Johdon ohjaus.
2. Tietoturvallisuuden organisointi (7)
    - Sisäisen organisaatio, mobiililaitteet ja etätyö.
3. Henkilöturvallisuus (6)
    - Työsuhteen alussa, aikana, muuttuessa ja päättyessä.
4. Suojattavan omaisuuden hallinta (10)
    - Vastuut, tietojen luokittelu, tietovälineiden käsittely.
5. Pääsynhallinta (14)
    - Liiketoiminnalliset vaatimukset, pääsyoikeuksien hallinta, käyttäjän vastuut, järjestelmät ja sovellukset.
6. Salaus (2)
    - Hallinta.
7. Fyysinen ja ympäristön turvallisuus (15)
    - Turva-alueet, laitteet.
8. Viestintäturvallisuus (7)
    - Verkon turvallisuus, tietojen siirtäminen.
9. Käyttöturvallisuus (14)
    - Toimintaohjeet ja velvollisuudet, haittaohjelmilta suojautuminen, varmuuskopiointi, kirjaaminen ja seuranta, ohjelmistot, haavoittuvuuksien hallinta, auditoinnit.
10. Järjestelmien hankkiminen, kehittäminen ja ylläpito (13)
    - Turvallisuusvaatimukset, kehitys- ja tukiprosessit, testiaineistot.
11. Suhteet toimittajiin (5)
    - Tietoturva toimittajasuhteissa, palveluiden hallinta.
12. Tietoturvahäiriöiden hallinta (7)
    - toimintamalli.
13. Liiketoiminnan jatkuvuuden hallinta (4)
    - Tietoturvallisuuden jatkuvuus, vikasietoisuus.
14. Vaatimustenmukaisuus (8)
    a. Lainsäädäntö ja sopimukset, katselmoinnit.

ISO 27001 sisältää yhteensä 14 kategoriaa, 35 aluetta ja 114 aihetta (PIRHONEN, 2018.)

2.4 Tietoturvan mittaaminen ja johtaminen organisaatiossa

Tietoturvan mittaaminen voidaan jakaa karkeasti kolmeen eri tasoon: strategiseen, taktiseen ja operatiiviseen (KUVA 7).



Kuva 7. Kuvassa on tietoturvan mittaamisen tasot jaettuna kolmeen päätasoon. (PIRHONEN, 2018).

Strategisella tasolla keskeiset kysymykset liittyvät tietoturvatason riittävyyteen ja riskien hallintaan. Lisäksi strategisella tasolla mietitään tietoturvapanostuen oikeaa kohdentamista ja niistä saatavaa hyötyä. Strategisen tason määrittelystä vastaa käytännössä toimitusjohtaja, johtoryhmä, hallitus.

Taktisella tietoturvatasolla mietitään, onko yrityksen prosesseissa ja projekteissa huomioitu riittävällä tasolla tietoturva. Taktisella tietoturvatasolla tietoturvaratkaisut toimivat keskeisen liiketoiminnan tukena. Taktisen tason määrittelystä vastaa yksitöiden ja toimipaikkojen johtoryhmät.

Operatiivisella tasolla tarkastellaan tietoturvaprosessien ja tietoturvaratkaisujen toimivuutta käytännön tasolla. Keskeisessä roolissa on tietoturvaratkaisujen toimivuus ja tehokkuus osana organisaation toimintaa. Operatiivisen tason määrittelystä ja seurannasta vastaa prosessien, tuotteiden ja palveluiden omistajat. (PIRHONEN, 2018.)

2.5 Tietoturvatasot käytännössä

Tietoturvan hallinta alkaa strategiselta tasolta (KUVA 8), jossa yhdessä johdon kanssa tunnistetaan omaan yritystoimintaan liittyvät korkeimmat tietoturvariskit. Tietoturvan hallinta vaatii aina resursointia, niin henkilöiden, rahan ja ajan suhteen. Budjettiin tulee varata riittävästi rahaa, jotta tietoturvaa voidaan laadukkaasti hallita. Johdon tulee varmistaa, että toiminta täyttää vaatimuksenmukaisuuden ja ymmärtää oman yrityksen tilanne suhteessa muihin toimijoihin samalla toimialalla. Vakavat tietoturvapoikkeamat tulee tunnistaan ja niihin varautuminen tulee olla jatkuvan parantamisen mallin mukaista toimintaa.

Prosessit ja järjestelmäkehitys tasolla määritetään tarkemmin, kuinka tietoturvaa hallitaan enemmän käytännön tasolla. Strategisella tasolla määritetyt määritellyt korkean potentiaalin tietoturvariskit pilkotaan pienempiin kokonaisuuksiin ja niille määritellään hallintakeinot. Toimintaan ja järjestelmään testataan erilaisilla testausmenetelmillä, muun muassa penetraatio -testauksella, jossa järjestelmään yritetään hallitusti hyökätä ja tällä voidaan testata organisaation puolustuskykyä ja valmiutta palautu mahdollisesta tietoturvaloukkauksesta.

Varsinainen tietoturvan operatiivinen taso on tietoturvan operointi, jossa seurataan tietoturvan toteutumista käytännössä. Tärkeimpiä seurattavia mittareita ovat tietoturvapoikkeamien lukumäärä, tyyppi, toimenpiteet ja poikkeamien käsittelyaika sekä tila. Poikkeamiin tulee reagoida viipymättä ja korjaavat toimenpiteet tulee aloittaa heti niiden määrittelystä. Tietoturvahenkilöstön tukena on käytössään järjestelmiä, jotka seuraavat verkon tilaa ja siihen kohdistuneita hyökkäysyrityksiä. Tietoturvan laadukas hallinta edellyttää valveutuneisuutta henkilöstöltä. Henkilöstön valveutumisen lisäämiseksi on järjestettävä tietoturvakoulutusta ja käytännön esimerkein tuoda esille tietoturvan merkitys omassa organisaatiossa. Tietoturva on niin vahva, kuin sen heikoin lenkki.

Kuva 8. Tietoturvan tasot käytännössä. (PIRHONEN, 2018.)

3 DIGITAALISEN TURVALLISUUDEN PROSESSIT

3.1 Osaamisen soveltaminen muuttuvassa ympäristössä

Tietoturva on laaja käsite, joka pitää sisällään neljä turvallisuuden kokonaisuutta: kyberturvallisuus, digitaalinen turvallisuus, tietoturvallisuus sekä tietotekninen turvallisuus. Näistä jokainen tavoittelee samaa turvallisuuden päämäärää, mutta käyttävät sen saavuttamiseksi toisistaan poikkeavia menetelmiä ja reittejä (KUVA 9).

3.1.1 Kyberturvallisuus

Kyberturvallisuus keskittyy yhteiskunnan kriittisten toimintojen keskinäisriippuvuuteen, toimivuuteen ja verkottuneen toimintaympäristön tietoturvallisuuteen kokonaisuutena. Kyberturvallisuuden fokus on yhteiskunnan toimivuuden varmistamisessa.

3.1.2 Digitaalinen turvallisuus

Digitaalinen turvallisuus korostaa digitalisoitumisen, automatisoinnin, teollisen internetin, esineiden internetin ja niistä johtuvien liiketoiminnan ja toimintamallien muutoksen vaikutuksia tietoturvallisuuteen. Digitaalisen turvallisuuden fokus on (tietoturva)toimintatapojen muutoksessa.

3.1.3 Tietoturvallisuus

Tietoturvallisuus huomioi tietojen suojaamisen laaja-alaisesti riippumatta tiedon olomuodosta, sijainnista tai käsittelytavasta. Kokonaisvaltainen näkökulma huomioiden organisaation tavoitteet, ihmiset, prosessit, teknologian ja ulkoiset riippuvuudet. Tietoturvallisuuden fokus on organisaation sekä sen palvelujen, prosessien ja tietojen suojaamisessa.

3.1.4 Tietotekninen turvallisuus

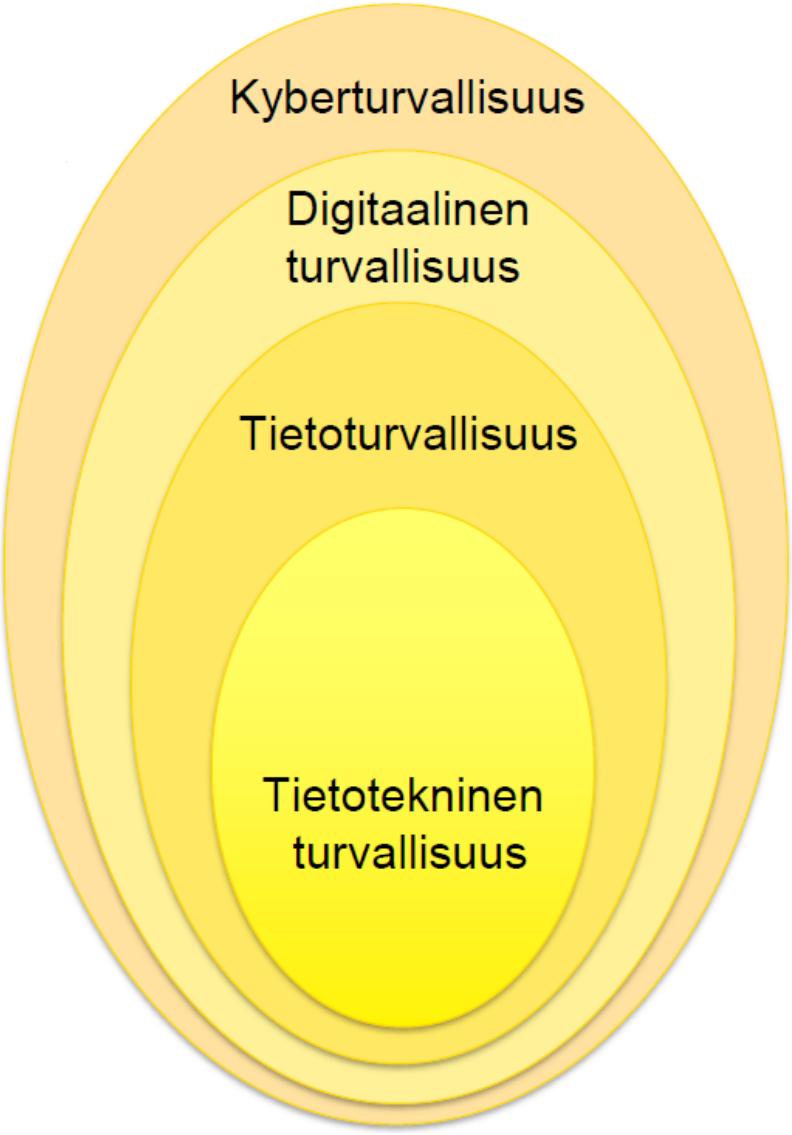
Tietotekninen turvallisuus (It-turvallisuus, ICT-turvallisuus) keskittyy tietojen, tietojärjestelmien ja tietoverkkojen tekniseen suojaamiseen. Tietoteknisen turvallisuuden fokus on teknisissä ratkaisuissa, tietoturvatuotteissa ja teknisessä osaamisessa. (PIRHONEN, 2018.)

Termistö laajenee entisestään, mikäli joukkoon otetaan mukaan sotilaallinen näkökulma. Kaikki valtiot ovat varautuneet puolustamaan kansalaisiaan sekä aluettaan sotilaallisen vaikutuskeinoin. Laajamittainen tietotekniikan käyttö on altistanut valtioita haavoittuvuuksille, tästä syystä tietojärjestelmien puolustaminen ulkoisia hyökkäyksiä vastaan on vähintäänkin yhtä tärkeää kuin maan rajojen aseellinen puolustaminen.

Verkko eroaa perinteisestä taistelukentästä sillä, että siellä ei ole maantieteellisiä rajoja, mutta kaikki valtiot haluat päättää toimistaan ja asioistaan itsenäisesti, ilman että mikään ulkovaltio uhkailee, painostaa tai suoranaisesti hyökkää. Yksikään valtio ei halua, että sen kansalaisiin yritetään vaikuttaa

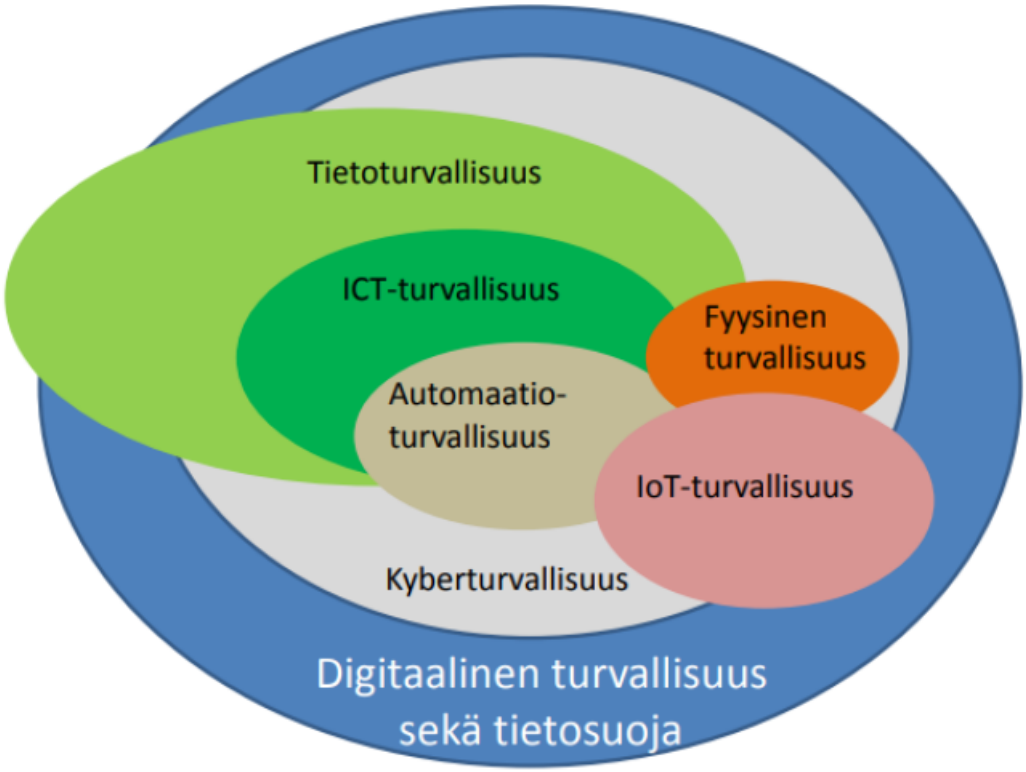
epärehellisin keinoin tai että valtion päätöksentekoa pyritään vakoilemaan tietoverkkojen avulla. (JÄRVINEN, Esitysmateriaali, 2018).

”Samalla, kun pyrimme huolehtimaan omien tietojemme ja koneidemme turvallisuudesta, edistämme myös kansallista kyberturvallisuutta. Ja kääntäen: jos laiminlyömme henkilökohtaiset asiamme, vaarannamme koko Suomen tulevaisuuden” (JÄRVINEN, Kyberuhkia ja somesotaa, 2018, s. 14).



Kuva 9. Digitaalisen turvallisuuden toimintaympäristö. (PIRHONEN, 2018).

Loppukäyttäjät kohtaavat digitaalisessa turvallisuudessa usein kymmeniä erilaisia termejä, jotka aiheuttavat helposti hämäännystä, onkin tärkeää olla sotkeutumatta termeihin – soveltaminen omaan organisaatioon parantaa tiedon välittämistä ja ymmärtämistä omassa organisaatiossa. (PIRHONEN, 2018).



Kuva 10. Digitaalisen turvallisuuden yhteydet muihin toimintaympäristöihin. (PIRHONEN, 2018).

Yritysten ja yhteisöjen tulee ymmärtää digitaaliseen turvallisuuden laajuus ja se, että yksi ihminen ei pysty hallitsemaan kaikkia digitaalisen turvallisuuden osa-alueita (KUVA 10). Yarassa digitaalisen turvallisuuden vastuut on hajautettu eri organisaatioihin ja organisaatiotasoille, jotta tiedon ja osaamisen eheys saadaan säilymään. Mietittäessä suuren pörssiyhtiön digitaalista turvallisuutta, tulee laajentaa näkykulmaa koskemaan koko toimintaprosessia, eikä vain yksittäisiä käyttäjiä tai pieniä kokonaisuuksia. Turvallisuutemme on yhtä vahva kuin sen heikoin lenkki. (YARA, International ASA, 2019.)

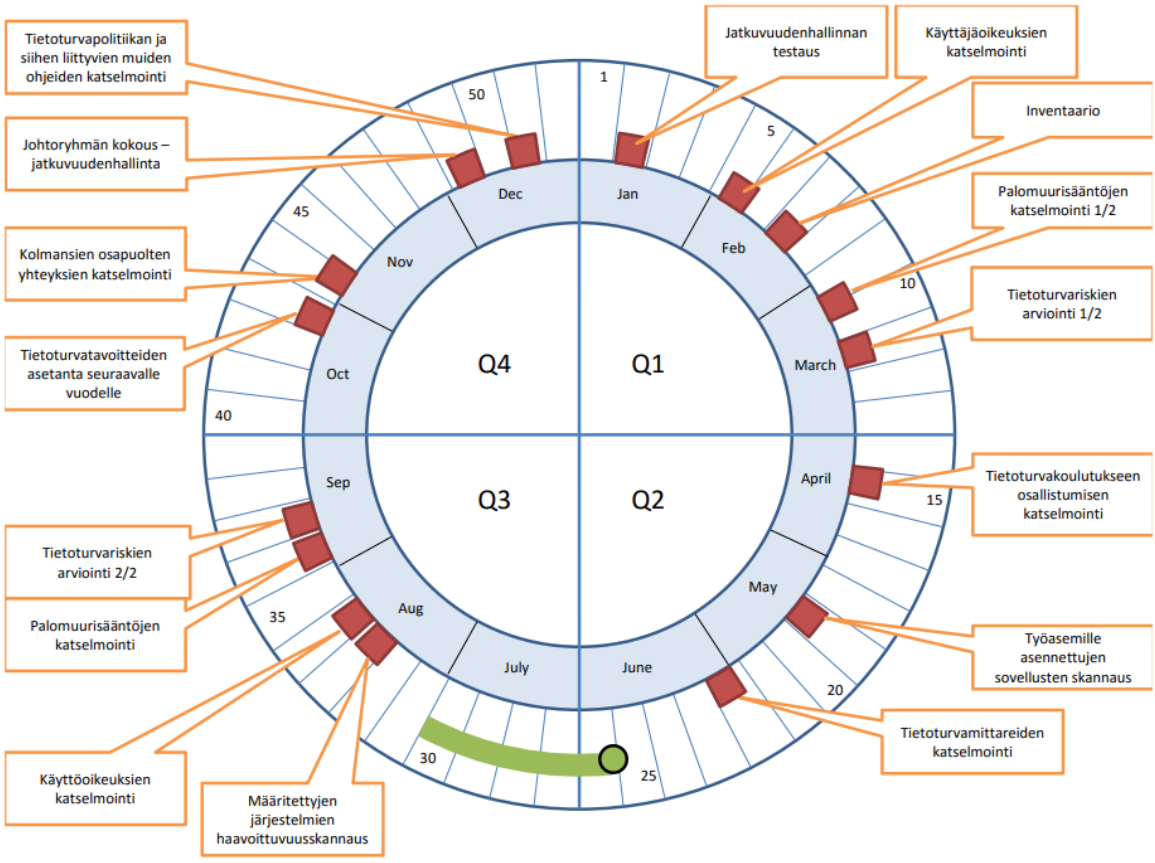
3.2 Roolit digitaalisessa turvallisuudessa

Yhdistäessämme digitaalisen turvallisuuden sekä tietosuojan saamme laajan joukon asioita ja prosesseja, johon meidän yrityksenä on pystyttävä vastaamaan. Kuten johdanto-osiossa viittasin Yaran esimerkkiin toimipaikkojen ja toimintojen verkottumisesta keskenään, on seuraavassa kuvassa (KUVA 11) esitetty digitaalisen turvallisuuden hallintaan tarvittavaa osaamista ja henkilöstä tehtävänimikkeittäin. Nimikkeet on pidettävä englanninkielisenä, jotta pystymme erottamaan eri turvallisuuden osa-alueet toisistaan. Turvallisuutta ei pidä ajatella yrityksessä kuluna, vaan panostuksena toiminnan eheyteen ja jatkumiseen.

Kuva 11. Digitaalisen turvallisuuden hallintaan tarvittavia rooleja (CYBER DEGREES, 2019).

3.3 Jatkuvien palveluiden hallinta

Jatkuvia palveluita tulee hallita prosessimaisesti. Tietoturvapolitiikan ja siihen liittyvän hallintamallia voidaan toteuttaa hyödyntäen tietoturvan vuosisuunnittelua. Johto vastaa siitä, että toimivalla organisaatiolla on riittävät resurssit käytössään, jotta he voivat hoitaa vuosittaiset ylläpitotehtävät ja toteuttaa kehittämistoimintaa annettujen valtuuksien puitteissa sekä vastata tarvittavasta budjetoinnista ja investointiesityksistä tietoturvanhallintaan liittyen. (VALTIONVARAINMINISTERIÖ, 2019.)



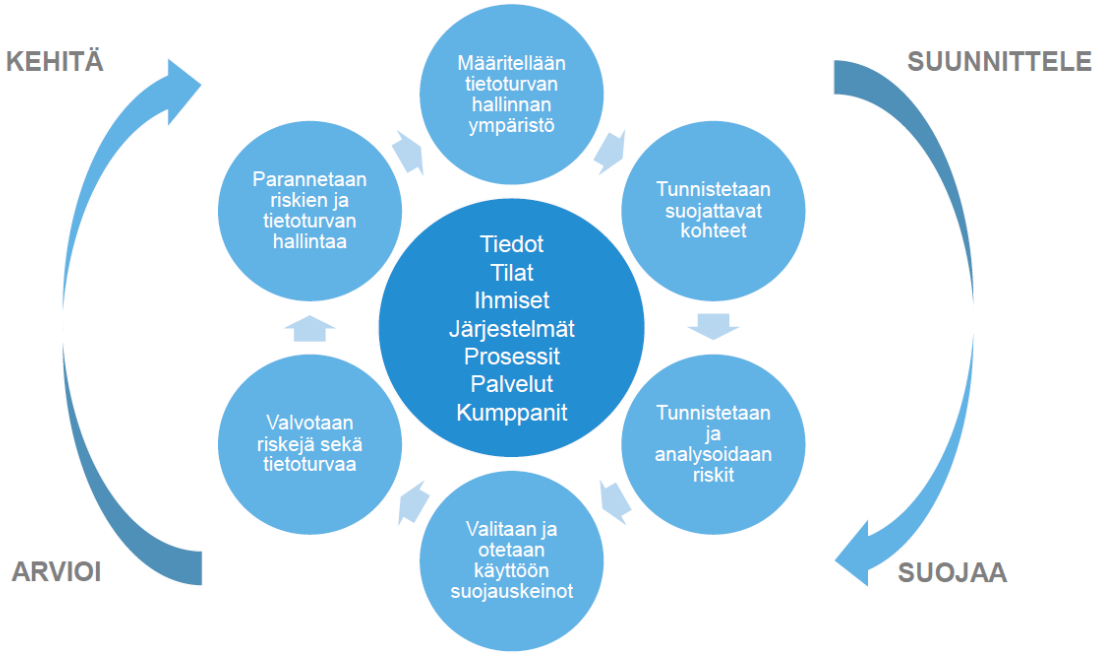
Kuva 12. Vuosikello tietoturvan hallinnassa. (KPMG, Tietoturvan hallinta, 2016).

Vuosikello (KUVA 12) on hyvä apuväline kuvaamaan jatkuvien palveluiden systemaattista hallintaprosessia. Vuosisuunnitelma sijoitetaan vuosikellon kehälle, jolloin voidaan suunnitelmallisesti varmistaa toiminnan taso. Vuosikello toimii hyvänä yleisaikanatauluna, josta tietoturvasta vastaava henkilö tekee tarkemmat suunnitelmat käytännön tehtäviä varten. Tietoturvan hallinta tulee olla jatkuvaa ja säännönmukaista.

3.4 Tietoturvallisuuden hallinta ja riskien arviointi

Digitaalisen turvallisuuden riskienarvioinneissa hyödynnetään Yaran omaa riskimatriisia. Digitaaliseen turvallisuuteen liittyvissä riskienarvioinnissa aiheuttaa haasteita kokemusperusteisen tiedon puute, jonka perusteella voidaan arvioida ja laskea riskiluku todennäköisyyden ja seuraukseen tulona. Taustatiedon vähyys aiheuttaa haasteita, mutta näissä riskienarvioinneissa tulee hyödyntää laaja-alaisesti automaatioturvallisuuden, fyysisen turvallisuuden ja tietoturvallisuuden kokemuksen omaavia henkilöitä. Riskienhallintaprosessi on kuvattu alla (KUVA 13).

Digitaalisen turvallisuuden riskienarviointia voidaan verrata työturvallisuudesta tutumpaan malliin. Riskejä ei koskaan voida kokonaan poistaa, vaan meidän täytyy tunnistaa mahdolliset vaaratekijät ja hallita ne siten, että toimintamme riski on hyväksyttävän alhaisella tasolla.



Kuva 13. Riskienhallintaprosessi digitaalisessa turvallisuudessa. (TIETO, 2019).

Riskienhallinta käytännössä tarkoittaa hallintakeinojen määrittämistä ja toteuttamista siten, että toistuvan tapahtuman todennäköisyyttä saadaan pienennettyä ja tapahtumasta aiheutuvaa seurausta lievennettyä. Kokonaisuudessaan riskien arviointi on osa riskienhallintaprosessia, johon kaikki turvallisuuden osa-alueet kuuluvat. Yaralla käytetään riskienhallintamenetelmänä priorisoitua listausta keinoista, jolla riskiä voidaan pienentää. (YARA, International ASA, 2019.)

Yaralla riskienhallinta perustuu suunnitelmalliseen riskien arviointiin, jonka tavoitteena on löytää merkittävät riskitekijät, jotta niihin voidaan varautua riittävillä toimenpiteillä ja saattaa riskit hyväksyttävälle tasolle. Riskien arvioinnissa ei tule keskittyä vain yksittäiseen suoritukseen, vaan riskien arvioinnissa tulee ottaa huomioon koko prosessi ja sen kaikki oheisprosessit.

Kun kaikki prosessiin tai tehtävään liittyvät vaaratekijät ovat tunnistettu, tulee jokainen vaara käsitellä omanaan ja sen aiheuttama riski on arvioitava kahdessa vaiheessa. Työriskien arviointitaulukko on esitetelty jäljempänä (KUVA 14).

Ensimmäisessä vaiheessa tulee arvioida, kuinka suuri riski vaarasta aiheutuu ilman lisättyjä hallintakeinoja. Kaikki hallintakeinot tulee jättää huomioon ottamatta riskienarvioinnin ensimmäisessä vaiheessa, jotta näemme alkuperäisen riskin ja voimme ymmärtää hallintakeinojen avulla saavutettavat hyödyt.

Toisessa vaiheessa arvioidaan riski hallintakeinojen käyttöönottamisen jälkeen. Mikäli riskitaso ei ole hyväksyttävällä tasolla, huolimatta hallintakeinoista, tulee meidän tunnistaa ja ottaa käyttöön turvallisuuttaparantavia toimenpiteitä. Näillä toimenpiteillä tulee saada pienennettyä seurausten vakavuutta tai vähentää tapahtuman toistumisen todennäköisyyttä. (YARA, International ASA, 2019.)

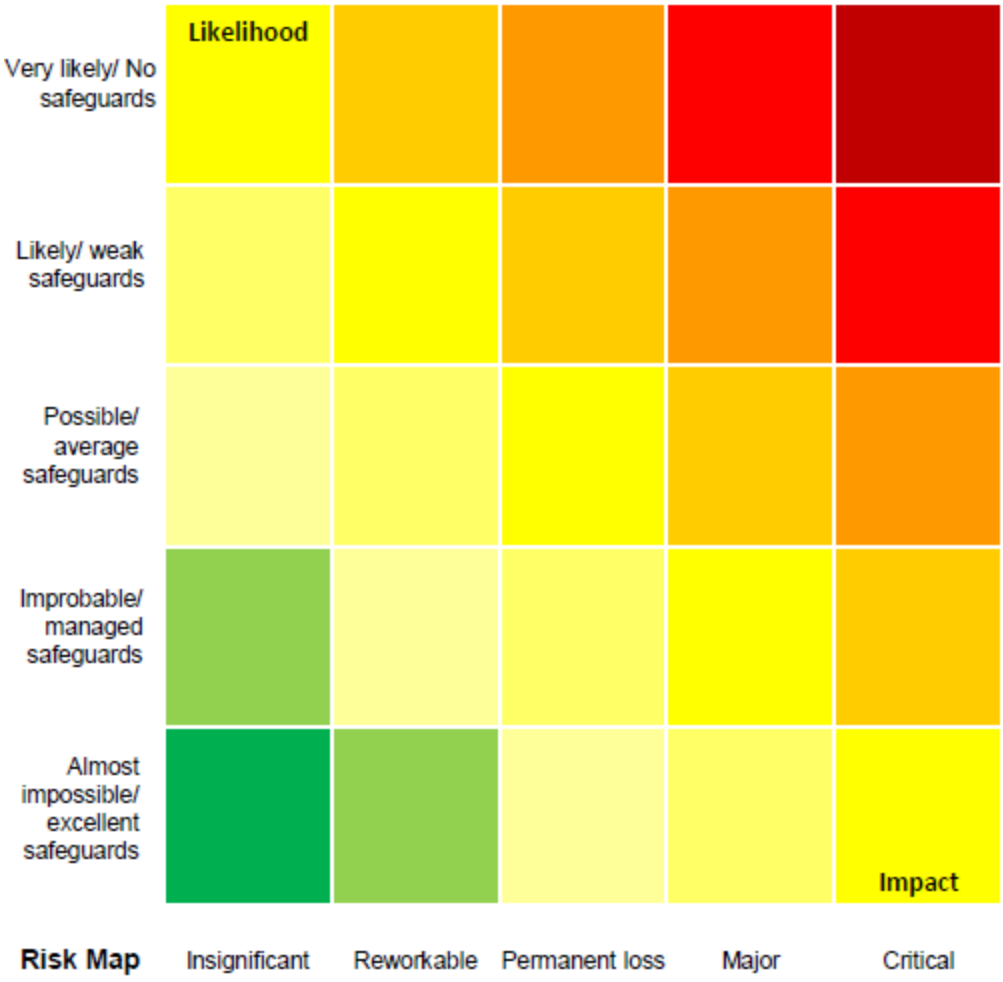
Työriskien arviointitaulukko				Todennäköisyys				
				Erittäin epä-toden-näköinen	Epätoden-näköinen	Mahdollista sattua	Toden-näköinen	Erittäin toden-näköinen
Vakavuus	Todella vakava	Useita kuolonuhreja	1					
	Suuri	Kuolema, vaikea vamma ja pysyvä haitta, krooninen työperäinen vakava sairaus	2					
	Keskisuuri	Vakava vamma, ei pysyvää haittaa Poissaolo >7 päivää	3					
	Pieni	Korvaavan työn tapaus tai lääkärinhoitoa vaatinut tapaus. Poissaolo <=7 päivää	4					
	Vähäinen	Ensiapua vaatinut tapaus	5					

Kuva 14. Yara 5x5 riskienarviointitaulukko työriskin arviointiin (YARA, International ASA, 2019).

Riskiluku lasketaan kertomalla seurausten vakavuus todennäköisyydellä. Tästä saadaan tuloksena riskin suuruus. Riski = seurausten vakavuus x todennäköisyys.

Projektitoiminnassa rakennetaan jatkuvasti uusia tuotanto- ja oheistiloja, joiden kokonaisturvallisuutta täytyy miettiä myös digitaalinen turvallisuus mielessä. Digitaalinen turvallisuus on otettava osaksi projektin riskienhallinta ja sitä on viestittävä jatkuvasti, jotta henkilöstön tietoisuus kasvaa asian suhteen. (YARA, International ASA, 2019.)

Seuraavassa kuvassa (KUVA 15) on malliesimerkkinä 5x5 riskimatriisi, joka on sovellettu digitaalisen turvallisuuden riskien arviointiin.



Kuva 15. 5x5 riskienarviointitaulukko digitaaliseen turvallisuuteen (KPMG, Esitysmateriaali, Pauli Wihuri, 2019)

3.5 Esimerkkejä mahdollista riskeistä

1. Kriittisen / salaisen tiedon vaikutus vaihtelee sen arvovirran mukaisesti. Aiheuttaa taloudellisia, markkinaosuus- ja voittomarginaalitappioita, jotka johtuvat digitaalisista virheistä tai ulkoisista / sisäisistä verkkohyökkäyksistä.

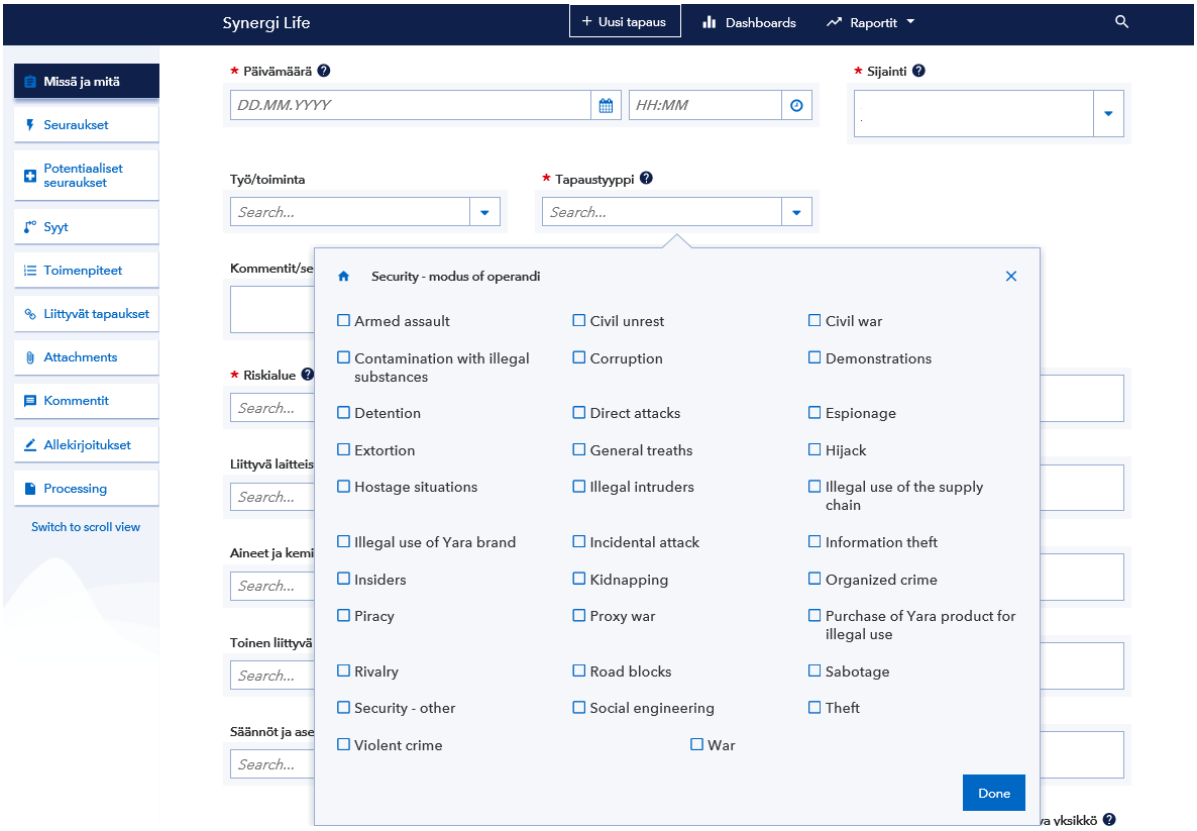
2. Tuotannon ja tuotetoimitusten keskeytykset aiheuttavat vaaraa, joka aiheuttaa taloudellisia ja asiakasuskollisuuden menetyksiä digitaalisten virheiden tai ulkoisten / sisäisten verkkohyökkäyksien takia.

3. Digitaalisen omaisuuden menetys digitaalisen omaisuuden luvattoman siirron vuoksi. Epäsuora menetys, joka johtuu tapahtumien reagoinnin hitaudesta ja virheistä, vahinkojen vähentämisestä, reagoinnista ja liiketoimintaa keskeyttävistä siirroista.
4. Digitaalinen muutos ja häiriö kehityksessä, joka johtuu epäonnistuneesta digitaalimuutoksesta digitaalisten palveluominaisuuksien kehittämiseen / käyttöönottoon liittyen. Hidas tai kykenemätön organisaatio ei kykene vastamaan asiakkaan digitalisaation tarpeisiin.

5. Yhtäkkinen strategisen digitalisaatiokumppanin menettäminen. (KPMG, Tietoturvan hallinta, 2016.)

3.6 Turvallisuuspoikkeamien hallinta

Yaralla turvallisuuspoikkeamien hallintajärjestelmänä toimii DNV toimittama Synergi Life raportointiympäristö (KUVA 16). Turvallisuuspoikkeamien kirjaaminen, tutkiminen ja toimenpiteiden vastuuttaminen tulee olla läpinäkyvää ja järjestelmän varassa – ihmisen muisti on rajallinen ja ilman ulkopuolista ärsykettä asiat monesti jäävät tekemättä. Periaatteella ”se mitä valvotaan, tulee myös tehdyksi” on hyviä ja kauaskantoisia seurauksia. (YARA, International ASA, 2019.)



Kuva 16. Kuvakaappaus Synergi Life raportointijärjestelmästä. (YARA, International ASA, 2019).

4 DIGITAALISEN TURVALLISUUDEN HALLINTA

4.1 Tietoturvan pelisäännöt työpaikalla ja kotona

Tietoturvan hallinta ei ole vaikeaa, se on pieniä loppukäyttäjän tekoja tai useimmin tekemättä jättämisiä. Petteri Järvinen on koostanut teoksessaan Kyberuhka ja somesotaa viiden yksinkertaisen ohjeen muistisäännön, jonka avulla torjut valtaosan kaikista tietoturvaongelmista ja kyberhyökkäyksistä.

1. Noudata salasanahygieniaa
    - Salasanan pitää olla riittävän vahva eli mahdoton arvata ja vaikea murtaa.
    - Jokaiseen palveluun tulee keksiä eri salasana.
    - Kaksivaiheinen todennus (MFA) tulee ottaa käyttöön sitä tukevissa palveluissa.

2. Tunnista tiedonkalastelu
    - Ennen palveluun kirjautumista tulee varmistaa, että sivu on oikea ja yhteys on salattu (https).
    - Älä koskaan kirjaudu palveluun sähköpostiviestissä olevan linkin kautta.
    - Älä luovuta tietoja puhelimessa henkilölle, jota et tunne henkilökohtaisesti.

3. Ole varovainen tiedostoliitteiden käsittelyssä
    - Älä käynnistä dokumenttitiedoston makroja.
    - Jos epäilet liitettä, avaa se älypuhelimella.

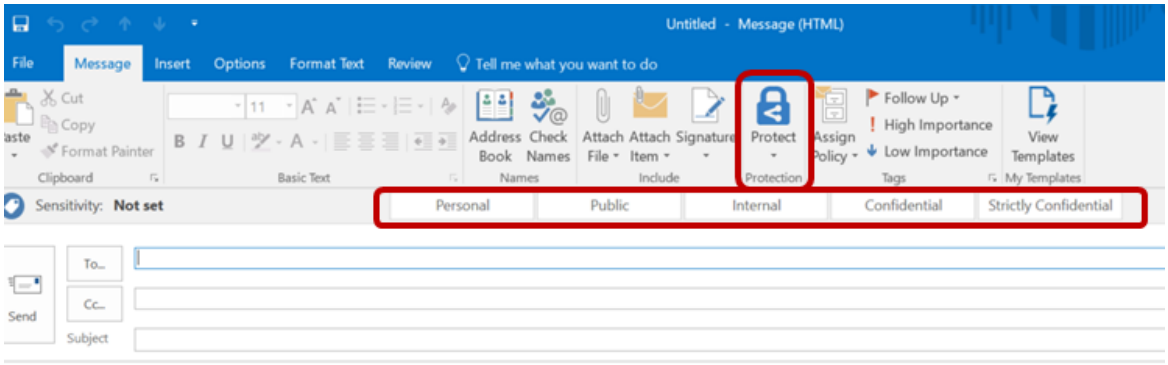
4. Päivitä laitteet ja ohjelmat
    - Päivitä keskeiset ohjelmat säännöllisesti.
    - Varmista, että klikkaat vain aitoja päivitysilmoituksia.

5. Älä kytke vieraita usb-laitteita koneeseen
    - Älä anna ulkopuolisten laittaa usb-tikkua tietokoneeseesi.
    - Rajoita omienkin tikkujen käyttö minimiin.
    - Käytä matkalla vain omaa laturiasi ja latausjohtoasi.

Erityistä varovaisuutta vaaditan johtajilta sekä HR- ja IT-osastojen työntekijöiltä. (JÄRVINEN, Kyberuhkia ja somesotaa, 2018.)

4.2 Sähköpostin turvallinen käyttäminen

- Käytävä internetiä ja sähköpostia vain hyväksytyillä tavoilla
  - Älä käytä sähköpostia tietojen tallentamiseen. Tallentamista varten käytössä on OneDrive for Business ja SharePoint!
  - Suoja arkaluontoiset asiakirjat ja sähköpostit Azure Information Protection (AIP)-työkalulla, esimerkki suojaustoimista alla olevassa kuvassa (KUVA 17).
  - Merkitse sähköpostit henkilökohtaiseen käyttöön.
  - Opettele tunnistamaan tietojenkalastelun merkkejä sekä tunnistamaan haitallisia sähköposteja.
  - Älä avaa linkkejä tai liitetiedostoja tarkastamatta niitä ensin.
  - Ilmoita epäilyttävistä sähköposteista.



Kuva 17. Tietojen luokittelutyökalu sähköpostiohjelmassa. (YARA, Yara End User Policy, International ASA, 2019b.)

4.3 Tietojen luokittelu

Yarassa tiedot luokitellaan päätasolla julkiseksi tiedoksi ja ei julkiseksi tiedoksi.

- Julkista tietoa ovat tiedot, jotka ovat saatavilla:
    - Yaran yleisiltä www.yara.com, tai muilta Yaran virallisilta verkkosivuilta.
    - Jotka on tuotu julki Yaran viestinnän kautta, HR:n tai sijoitussuhteiden ylläpitäjien toimesta.
    - Jonkin kolmannen osapuolen tekemänä julkisesta lähteestä.
    - Esimerkkejä julkisesta tiedosta:
        - Lehdistötiedotteet
        - Markkinointimateriaali
        - Tuote-esitteet
        - Työnhakuilmoitukset
- Ei julkinen tieto jaetaan Yarassa kolmeen eri alaluokkaan (esimerkkejä ei julkisista tiedoista):
    - Sisäinen tieto:
        - Organisaatiokaaviot
        - Yrityksen johtamis- ja ohjausdokumentit
        - Koulutusmateriaalit
    - Luottamuksellinen tieto:
        - Kaupalliset sopimukset
        - Laskut
        - Budjetit
    - Erittäin luottamuksellinen tieto:
        - Julkaisemattomat taloudelliset raportit
        - Hallituksen materiaali
        - Strategiaan liittyvä materiaali (YARA, Yara End User Policy, International ASA, 2019b.)

4.4 Kannettavat tietokoneet tai pöytäkone

- Suojaa laitteesi Yaran tarjoamalla tietoturvaohjelmistolla.
- Yaran hallitsema kannettava tietokone tai pöytäkone:
  - Älä lykkää käyttöjärjestelmäpäivityksiä.
  - Lukitse aina tietokone, kun poistut sen luota, vaikka vain lyhyeksi ajaksi.
  - Älä jätä kannettavaa tietokonetta vartioimatta tai näkyville autossa, hotellihuoneessa tai julkisella paikalla.
  - Älä aseta tuntematonta USB-muistitikkua tarkastamatta sitä ensin virustorjuntaohjelmalla.
  - Jos sinun on tallennettava arkaluontoisia tietoja USB-muistitikulle, varmista ensin, että tiedot on suojattu ja että USB-muistitikku on salattu.
  - Kirjaudu ulos tietokoneelta tai sammuta se, kun poistut sen luota pidemmäksi aikaan. Näin tietokoneen luvaton käyttö on vaikeampaa. (YARA, Yara End User Policy, International ASA, 2019b.)

4.5 Matkapuhelimet ja tabletit

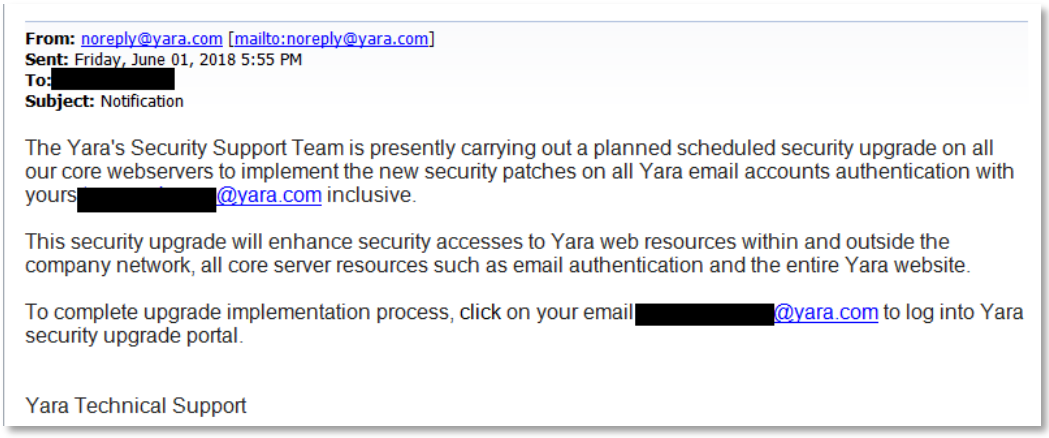
- Kirjaudu Yaran mobiililaitteiden hallintaratkaisuun (Intune).
- Käytä mahdollisuuksien mukaan PIN-koodia/salasanaa ja biometrisiä tietoja (esim. sormenjälki tai kasvotunnistus).
- Päivitä aina uusimpaan laitevalmistajan tukemaan käyttöjärjestelmäversioon.
- Älä asenna ohjelmistoa, jota ei ole hyväksytty laitevalmistajan virallisessa sovelluskaupassa.
- Älä anna Yaran hallitsemia mobiililaitteita muiden käyttöön, ei myöskään perheenjäsenten.
- Käytä Yaran hallitsemissa sovelluksissa mahdollisuuksien mukaan ylimääräisiä suojauksia, esim. Touch ID tai sormenjälki, kun käytät Yaran Outlookia mobiililaitteessa.
- Ilmoita välittömästi, jos laite katoaa (esim. häviää tai varastetaan), vaihda salasanani varotoimenpiteenä.
- Poista Wi-Fi, Bluetooth ja NFC käytöstä, kun niitä ei tarvita. (YARA, Yara End User Policy, International ASA, 2019b.)

4.6 Tietoturva työmatkojen ja etätyöskentelyn aikana

- Yaran laitteet on tarkoitettu Yaran työtehtävien hoitamiseen. Laitteita ei koskaan saa luovuttaa perheenjäsenten käyttöön!
- Pidä aina kaikki laitteet mukanasi käsimatkatavaroissa lennon aikana.
- Vältä arkaluontoisten tietojen käsittelemistä avoimissa ja suojaamattomissa verkoissa (käytä aina uskottavalla digitaalisella varmenteella suojattuja HTTPS-sivustoja).
- Vältä arkaluontoisesta sisällöstä puhumista ja sen käsittelemistä julkisissa paikoissa (käytä esimerkiksi mahdollisuuksien mukaan tietoturvasuojaa).
- Noudata ylimääräisiä suojaustoimenpiteitä matkustaessasi korkean riskin maihin. (YARA, Yara End User Policy, International ASA, 2019b.)

4.7 Digitaalisen turvallisuuden poikkeustilanteita

Maailmanlaajuisena toimija Yara on kohdannut lukuisia huijausyrityksiä digitaalisen turvallisuuden saralla. Esimerkkinä voidaan käyttää vuoden 2018 kesäkuun tapausta, jossa rikolliset onnistuivat tunnistamaan Yaran johtajia ja esimiehiä ja he lähettivät heille huijaussähköpostiviestejä. Sähköpostien väitettiin olevan peräisin Yaran teknisestä tuesta (KUVA 18), mutta todellisuudessa rikolliset yrittävät saada tietoonsa käyttäjänimiä ja salasanoja. Huijaussähköpostien kautta saamiensa tietojen avulla rikolliset onnistuivat saamaan yhteyden joihinkin asiakkaisiimme Yaraa esittäen.



From: noreply@yara.com [mailto:noreply@yara.com]
Sent: Friday, June 01, 2018 5:55 PM
To: [redacted]
Subject: Notification

The Yara's Security Support Team is presently carrying out a planned scheduled security upgrade on all our core webservers to implement the new security patches on all Yara email accounts authentication with yours[redacted]@yara.com inclusive.

This security upgrade will enhance security accesses to Yara web resources within and outside the company network, all core server resources such as email authentication and the entire Yara website.

To complete upgrade implementation process, click on your email[redacted]@yara.com to log into Yara security upgrade portal.

Yara Technical Support

Kuva 18. Esimerkki kalasteluyrityksestä. (YARA, International ASA, 2019.)

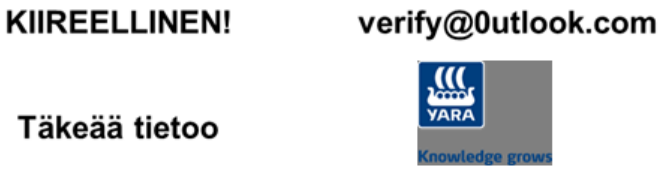
Tietojen kalastelu on yleistynyt viime aikoina paljon ja vuonna 2018 tavoitteenamme oli nostaa Yaran henkilöstön tietoisuutta liittyen tietojenkalasteluyrityksiin. Yarassa on tehty simuloituja tietojenkalasteluyrityksiä, jotta voimme selvittää kuinka moni työntekijä avaa haitallisia linkkejä ja antaa tunnistetietojaan epäilyttäville sivustoille. Alla olevassa kuvassa (KUVA 19) nähdään, että meillä on kokonaisuutena vielä paljon parannettavaa.

Kuva 19. Tuloksia simuloidusta kalastelukampanjasta. (YARA, International ASA, 2019).

Yara Suomen osalta tietojenkalasteluviestejä lähetettiin 2815 kappaletta. Linkkiä klikattiin 195 kertaa ja kirjautumistietonsa anoi jopa 101 käyttäjää. Suomessa voidaan siis hivenen nostaa hattua itsellemme, että olemme keskimääräistä paremmin orientoituneita digitaaliseen turvallisuuteen. (YARA, International ASA, 2019.)

4.8 Mitä tietoturvahäiriöt ja -loukkaukset ovat ja kuinka ne tunnistat?

- Tietoturvahäiriöitä tai -loukkauksia voivat esimerkiksi olla
  - Jokin Yaran tieto katoaa tai se kerrotaan luvattomille osapuolille tai näin epäillään tapahtuneen.
  - Salasanoja tai muita järjestelmään pääsyä hallitsevia mekanismeja katoaa, varastetaan tai paljastetaan tai niiden epäillään kadonneen, tulleen varastetuiksi tai paljastetuiksi.
  - Kaikki epätavallinen järjestelmän toiminta, kuten tiedostojen puuttuminen, toistuvat järjestelmän kaatumiset ja väärin reititetyt viestit.
  - Kaikki tietoturvaa koskevat hälytykset, varoitukset ja epäillyt haavoittuvuudet.
  - Yleisen tietosuoja-asetuksen (GDPR) loukkaukset, joista ilmoittaminen on lakisääteinen velvollisuus.
  - Tunnista mahdolliset tietoturvaloukkaukset ja -häiriöt ja ilmoita niistä viipymättä Yaran tietoturvatiimille:
    - Ole varovainen, jos sähköposti vaatii ”välitöntä huomiota”.
    - Tarkista lähettäjän sähköpostiosoite, onko se oikein kirjoitettu, näyttääkö se epäilyttävältä?
    - Onko viestissä kirjoitusvirheitä (KUVA 20)?
    - Tarkista Yaran logo ja yhteystiedot. Näyttääkö logo tavanomaiselta?



Kuva 20. Esimerkkejä kalasteluviestien muokkauksista. (YARA, International ASA, 2019.)

4.9 Miten toimia epäilyttävissä digitaalisen turvallisuuden tilanteissa?

Tärkein vaihe loppukäyttäjä on tunnistaa epäilyttävät ja normaalista poikkeavat tietojenkalastelu tai muut haitalliset viestit sekä yhteydenotot. Työntekijän odotetaan ilmoittavan havaituista tai epäillyistä tietoturvaloukkauksista ja -häiriöistä. Älä odota jonkun muun tekevän ilmoitusta puolestasi.

- Jos saat epätavallisen sähköposti koskien erityisesti muuttuneita maksutietoja, niin varmista viestin aitous soittamalla tai lähettämällä tekstiviesti henkilölle. Jos saamasi viesti ei ole aito, ilmoita siitä välittömästi Yaran Global Service Desk-tukipalveluun.

- Jos saat epätavallisen puhelun koskien Yaran IT-asioita, joka ei ole Global Service Desk-tukipalvelusta, lopeta puhelu välittömästi. Global Service Desk ei koskaan kysy salasanatietojasi puhelussa. Tee puhelusta ilmoitus Global Service Desk-tukipalveluun.

- Jos saat odottamattoman tekstiviestin tai muun viestin digitaalisissa viestintäpalvelusovelluksissa, ohita se, äläkä avaa mitään linkkejä tai lataa mitään sisältöä. (YARA, 2019b.)

5 TULOKSET JA JOHTOPÄÄTÖKSET

Tässä luvussa käsitellään Yara Suomi Oy Siilinjärven toimipaikan digitaaliseen turvallisuuden nykytilaa ja esitetään johtopäätöksenä havaintoja, jolla digitaalisen turvallisuuden tilaa toimipaikalla voidaan kehittää. Luvun lopussa on omaa pohdintaa opinnäytetyön prosessista ja lopputuloksesta.

5.1 Digitaalisen turvallisuuden nykytila ja kehitysmahdollisuudet

Yara Suomi Oy, Siilinjärven toimipaikan digitaalisen turvallisuuden nykytilan tarkastelussa käytettiin DNV:n Information Security Management Systemin itsearviointityökalua (LIITE 1), mikä antaa hyvän yleiskuvan järjestelmien turvallisuuden nykytilasta. Kriittisten järjestelmien kuten automaation osalta kaikki tarkastelun kohdat täyttyivät, mutta tarkastelua tehtiin laajemmin sisältäen toimistoverkon sekä muut IP-pohjaiset järjestelmät, jotta löydettiin soveltuvia kehitysalueita digitaalisen turvallisuuden kehittämiseen Yara Suomi Oy, Siilinjärven toimipaikalla.

Yaralla on käytössään ylimmän johdon hyväksymä tietoturvapolitiikka ja se on viestitty henkilöstölle sekä se on saatavissa helposti toimintajärjestelmästämme. Yaran dokumentit ovat osa YMS (Yara Management System) -järjestelmää. Järjestelmässä dokumenttien omistajuus, hyväksyjä, hyväksyntä päivämäärä ja seuraava arviointipäivä ovat dokumentoitu sekä järjestelmä muistuttaa omistajaa automaattisesti dokumentaation tarkastuksesta. Tarkastamme toimintaamme näitä politiikkoja vasten ylätasolla säännöllisesti, erikseen määriteltyjen auditointien muodossa. Toimipaikallamme tarkastuksia tehdään etenkin kriittisten järjestelmien osalta, mutta toimintaamme voisi kehittää lisää tekemällä kelpoisuustarkastuksia myös muihin kuin operatiivisiin järjestelmiin.

Yaralla on käytössään riskinarviointiin useita työkaluja, joilla digitaaliseen turvallisuuden riskejä arvioidaan. Yaran toimintaa ohjaa lainsäädännön lisäksi yrityksen omat HOPS-dokumentit, joilla tarkennetaan lainsäädäntöä sekä paikallisia ohjeistuksia. Turvallisuuden (security) riskienarviointia ohjaa etenkin Security Management, Physical Security ja Personnel Security -dokumentaatio. Yrityksellä on systemaattinen toimintatapa sovittaa toimintansa vastaamaan turvallisuusuhkien riskejä sekä todennäköisyyksiä. Toiminnan riskit on arvioitu ja niitä vasten on tehty toimenpiteitä, jotta kokonaisriski on saatu hyväksyttävälle tasolle.

Vastuiden jakaminen on yrityksessä hoidettu selkeällä vastuumatriisilla, mutta vastuut jakaantuvat usean eri organisaation kesken. Toimintamallin tulee tukea organisaatioiden välistä toimintaa, jotta voidaan varmistua kaikkien toimenpiteiden määrittämisestä ja toteuttamisesta. Yrityksellä on prosessimainen käytäntöä kokoontua vastuuhenkilöiden kesken ja tarkastaa toimintaa ohjeistuksia vasten. Yarassa kaikille järjestelmille ja ohjelmistoille on määritelty omistaja, joka vastaan kyseisten järjestelmien ylläpidosta ja muun muassa tietoturvapäivitysten ajamisesta järjestelmään. Uusia järjestelmiä käyttöönotettaessa kriittisille järjestelmille on määritelty selkeät vahvennustoimenpiteet muun muassa USB -porttien deaktivointi ja ylimääräisten porttien sulkeminen.

Digitaalisen turvallisuuden hallinnassa yhdeksi kriittisimmistä tekijöistä on tunnistettu henkilöstön osaaminen. Yrityksessä on määritelty pakolliset tietoturvallisuuskoulutukset kaikille uusille henkilöille, sekä jo olemassa olevalle henkilöstölle, jotka ovat olleet työssä koulutuksen julkaisuajankohtana. Yrityksen tulisi panostaa myös digitaalisen turvallisuuden koulutuksen osalta jatkuvaan parantamiseen ja nostaa vuosittain päivitettävään turvallisuusperehdytykseen lisää digitaalisen turvallisuuden elementtejä.

Yaralla on käytössää aktiivinen tietoturvauhkien tunnistusohjelma, jossa henkilöstön valmiutta testaamaan muun muassa sähköpostitse lähetettävillä kalasteluviesteillä. Kalastelukampanjoiden tulokset julkaistaan aina koko yrityksen henkilöstön nähtäville ja uusittaessa kalastelukampanjaa henkilöstömme valmius tunnistaa kalasteluyrityksiä on parantunut merkittävästi.

Yara Siilinjärven toimipaikalla työskentelee yhteistyökumppaneita päivittäin lähes yhtä paljon kuin omia työntekijöitä. Vuoden tarkastelujakson aikana toimipaikallamme luvitetaan noin 3000 henkilöä. Tämä tarkoittaa sitä, että myös ulkopuolisten koulutukseen on panostettava enemmän. Vuoden 2020 perehdytysmateriaaliin on lisätty myös toimintaohjeita- ja malleja liittyen digitaalisen turvallisuuteen. Ulkopuolisilta, joilla on pääsy Yaran järjestelmiin, edellytetään aina salassapitosopimuksen allekirjoitusta ja samassa yhteydessä toimitetaan tietoturvaohjeet. Myös oma henkilöstö allekirjoittaa työsopimuksen myötä salassapitosopimuksen.

Yaralla on käytössään raportointimenettelyt, kuinka toimia mahdollisessa tietoturvapoikkeamassa tai muissa tietoturvan loukkausyrityksissä. Raportointijärjestelmä on käytössä omalle henkilöstölle ja niille ulkopuolisille henkilöille, keillä on pääsy Yaran järjestelmiin. Järjestelmän tietoisuutta ja toimintamallia tulisi kuitenkin korostaa enemmän, jotta järjestelmän käytettävyys olisi tiedossa mahdollisessa poikkeamatilanteessa. Raportointi tapahtuu tehokkaasti yrityksen tietoturvan keskusorganisaatiolle, mutta tiedottaminen ja raportointimalli loppukäyttäjille ei tavoita kaikkia kohtuullisessa ajassa. Kehityskohteena olisi tehostaa viestimistä eri organisaatioiden välillä.

Varautuminen kyberturvallisuuspoikkeamiin yrityksessä on hyvällä tasolla. Käyttäjillä itsellään ei ole oikeuksia asentaa ohjelmistoja tietokoneisiin ja sallituista ohjelmista on olemassa listaukset sekä portaali, josta IT-osasto ohjelmia voi asentaa. Järjestelmiä turvaamaan on rakennettu asianmukaiset haittaohjelmien tunnistamiseen ja automaattiseen poistamiseen tarkoitetut järjestelmät sekä toiminnallisuudet. Kaikki järjestelmät on suojattu asianmukaisilla suojauksilla muun muassa palomuurit ja IDS. Turvallisuuslokien seuranta painottuu kriittisiin järjestelmiin, joista saadaan automaattisesti ilmoituksia mahdollisista hyökkäysyrityksistä.

Yrityksellä on toiminnanjatkuvuussuunnitelma kriittisten järjestelmien ja komponenttien osalta. Varmuuskopiointi sekä niiden ylläpito on varmennettu asianmukaisesti. Ei kriittisten järjestelmien osalta palautumissuunnitelma ei ole riittävällä tasolla ja kehitysalueena on laajentaa suunnitelmat koskemaan myös ei kriittisiä järjestelmiä. Etukäteen mietityt resurssit sekä toimintasuunnitelmat nopeutta

palautumista huomattavasti mahdollisessa poikkeustilanteessa ja se tuo merkittäviä säästöjä, kun alhaalla olo aika saadaan pienennettyä minimiin. Kriittisten toimintojen osalta varautumissuunnitelmia testataan ja päivitetään, mutta toimintaa tulisi laajentaa myös muihin järjestelmiin.
Paikallinen IT-henkilöstö seuraa ja velvoittaa järjestelmien omistajia hallitsemaan lisenssien voimassaoloaikaa. Yrityksessä ylläpidetään päivitettyä lisenssirekisteriä, jotta kaikkien järjestelmien lisenssit ovat voimassa ja näin ollen järjestelmät ovat oikeutettuja niille kuuluviin tietoturvapäivityksiin. Toimipaikalla on myös käytössä prosessimainen auditointikäytäntö, jolla varmistetaan ohjelmistojen ja järjestelmien käyttöä.

Toimipaikalla on tunnistettu yrityksen toiminaan liittyvä ydintieto, joka on suojattu ja niitä koskevat järjestelmät ylläpidetty asianmukaisin käytäntein. Yrityksellä on ohjeet ja toimintamalli, kuinka tietoja tulee säilyttää, arkistoida ja poistaa. Kasvavien datamäärien seurauksena vanhentuneen ja ”turhan” tiedon poistaminen korostuu, jotta tärkeä ja tarpeellinen data saadaan käyttöön ketterästi. Henkilökunnalle tulee järjestää koulutusta, kuinka dataa toimipaikalla tulee hallita. Yrityksellä on myös järjestelmiä, jotka havaitsevat tärkeän tiedon siirtoyrityksiä ulos muihin kuin Yaran hallitsemiin palveluihin.

Yaralla on selkeä ja hallittu malli käsitellä henkilötietoja. Tarpeelliset henkilötiedot on tunnistettu ja niille on määritetty käyttötarkoitus. Yrityksellä on ohjeet ja toimintamalli, kuinka käsitellä henkilötietoja. Yrityksen tietojenkäsittely vastaa tietosuojalain 1050/2018 mukaisia vaateita sekä yleisen tietosuoja-asetuksen asettamia vaateita. Tietosuoja asioissa yritys on viestinyt henkilöstölleen ja yhteistyökumppaneilleen avoimesti toimintamalliansa ja korostanut tietosuojan merkitystä yrityksen toiminnassa.

Yhteenvetona löydetyistä (TAULUKKO 1) parannuskohteista nousee esille henkilökunnan koulutuksen lisääminen, kolmansien osapuolten huomioiminen digitaalisen turvallisuuden koulutuksissa sekä palautumissuunnitelmien syventäminen ja toimintamallin harjoittelu käytännössä.

Taulukko 1. Kehitysalueet ja toimenpiteet digitaalisen turvallisuuden parantamiseksi.

Kehitysalue	**Toimenpide**	**Kenen vastuulla**
Henkilökunnan koulutus	Digitaalinen turvallisuus tulee lisätä osaksi henkilökunnan vuosittain läpikäytävään turvallisuuden yleisperehdytykseen. Koulutuksessa on tärkeä huomioida käytännön läheisiä toimia digitaalisen turvallisuuden parantamiseksi ja hyödynnettävä yrityksen poikkeamaraportteja, joiden pohjalta materiaaliin luodaan todenmukaisia skenaarioita.	Turvallisuusorganisaatio
Kolmansien osapuolien koulutus	Digitaalinen turvallisuus tulee lisätä osaksi yhteistyökumppanien vuosittain läpikäytävään turvallisuuden yleisperehdytykseen. Koulutuksessa tulee painottaa urakoitsijan velvollisuuksia digitaaliseen turvallisuuteen, kuten: USB-tikkujen käyttö, dokumenttien luottamuksellisuus, omien tietokoneiden käyttäminen, liittyminen toimipaikan verkkoympäristöön.	Turvallisuusorganisaatio ja IT
Palautumissuunnitelmat	Toimipaikalle tulee luoda palautumissuunnitelmat myös ei kriittisille järjestelmille ja huomioida niissä varmuuskopiointi sekä niistä palauttaminen mahdollisessa digitaalisen turvallisuuden hyökkäyksessä. Palautumissuunnitelmat tulee luoda jatkuvan parantamisen malliin ja ne tulee tämän mukaisesti tarkastaa ja päivittää määräajoin.	Security Engineer, IT ja Digital Development Manager

Toimintamallit palautumisessa	Palautumissuunnitelmien lisäksi tulee luoda toimintamalli, kuinka palautuminen tehdään käytännössä. Toimintamallia tulee harjoitella säällisin määräajoin ja harjoitusten pohjalta toimintamallia tulee kehittää. Toimintamallit tulee säilyttää siten, että pääsy niihin on vain rajatulla henkilöstöllä ja siten, että ne ovat saatavilla mahdollisessa digitaalisen turvallisuuden hyökkäystilanteessa.	Security Engineer, IT ja Digital Development Manager

5.2 Pohdinta

Syvennettyäni tarkemmin Yara Suomi Oy, Siilinjärven toimipaikan digitaaliseen turvallisuuteen havaitsin, kuinka palasiksi kokonaisuudet on rikottu. Vastuut eri organisaatioille on jaettu: IT-osasto sekä automaatio vastaavat kyberturvallisuudesta ja tietosuojasta, paikalliset turvallisuusorganisaatiot vastaavat fyysisestä turvallisuudesta, rakennusosasto rakennuksien suunnittelusta, projektitoiminnot projektien hallinnasta ja niihin liittyvistä riskinarvioista. Turvallisuus on teema, joka kulkee jokaisen toiminnon mukana ja sen merkitys toiminnan turvaamiseen on kaiken lähtökohta.

Digitaalisen turvallisuuden hallinta edellyttää nyt ja etenkin tulevaisuudessa henkilöstöltä merkittävää osaamista ja valppautta tunnistaa sekä toimia oikein mahdollisissa digitaalisen turvallisuuden uhkatilanteissa. Tietoturvauhka voi odottaa aamulla työpöydällä USB-tikun muodossa, sähköpostissa kiinnostavana ”hei olet voittanut arvonnassa” -linkkinä tai vaikka kesken normaalin kokouksen, kun päivän puhuja haluaa siirtää koneellesi esityksenä. Lähtökohtaisesti oletamme Yaralla ja Yarelle työskentelevien toimivan yhtiön pelisääntöjen mukaisesti ja haluamme uskoa, että he työskentelevät meidän parhaaksemme – meidän kuitenkin tulee muistaa realiteetit ja olla varuillamme, jotta tietopääomamme sekä tuotantomme ovat turvassa.

Yara Siilinjärvellä on siirrytty puhumaan digitaalisesta turvallisuudesta ja tämän alle on niputettu yhdeksi kokonaisuudeksi näiden asioiden hallinta. Digitaalisen turvallisuuden dokumenttien kokoaminen ja soveltaminen omaan toimipaikkaamme on meneillään, mutta tärkeintä on, että tahtotilamme on määritelty ja pääsemme aloittamaan toimemme turvallisten tähtien alla.

Yksinään mikään näistä toimista ei mahdollista yrityksen turvallista jatkuvuutta, mutta yhdessä ne muodostavat kokonaisuuden, joka luo jatkuvuuden jo 50-vuotta jatkuneelle teemallemme ”Kivestä leipää ennen, nyt ja tulevaisuudessa!” (YARA, 50 vuotta juhlamateriaali, Yara Suomi Oy, 2019).

6 YHTEENVETO

Opinnäytetyön tavoitteena oli selvittää Yara Suomi Oy, Siilinjärven toimipaikan digitaalisen turvallisuuden nykytilaa ja etsiä parannuskeinoja, joilla digitaalisen turvallisuuden tilaa voidaan nostaa. Opinnäytetyöprosessi alkoi perehtymällä digitaalisen turvallisuuden teoriataustaan, etsimällä aiheeseen soveltuvaa kirjallisuutta, lakeja, standardeja sekä Yaran olemassa olevaa digitaalisen turvallisuuden materiaalia. Perehdyttyäni materiaaleihin huomasin, että Yaran käytössä oleva materiaali on yleisellä tasolla olevia toimintaohjeita loppukäyttäjille. Tavoitteena oli tuoda yrityksen henkilöstölle syvällisempää tietoa digitaalisen turvallisuuden johtamisesta, joten opinnäytetyöni alkuosa on teoriaan peilaavaa materiaalia.

Työn kappaleessa 1.4 herätellään lukijoita eli todellisia loppukäyttäjiemme digitaalisen turvallisuuden riskeihin ja korostetaan, miksi digitaalisen turvallisuuden hallinta on tärkeää. Tärkeys tiivistyy kahteen virkkeeseen: ”Kaikki kriittiset järjestelmät ovat suunniteltu jotain tiettyä toimintoa varten. Mikäli tämä toiminnallisuus katoaa järjestelmään kohdistuneen hyökkäyksen takia, voi sillä olla merkittäviä vaikutuksia tuotantoon, turvallisuuteen tai ympäristöön”. (BYRES, 2013).

Opinnäytetyön toisessa luvussa perehdytään tarkemmin teoriaperustaan ja lainsäädäntöön, jotka ohjaavat digitaalisen turvallisuuden johtamista. Luvussa käsitellään tietosuojaa ja siihen liittyviä vaikutuksia ja vastuita yritykselle sekä henkilöstölle. Yarassa korostetaan jatkuvan parantamisen toimintamallia ja sen soveltuvista digitaaliseen turvallisuuteen on avattu kappaleessa 2.3, jossa tarkastellaan jatkuvan parantamisen muotoon tehtyä ISO 27001 tietoturvallisuuden hallintajärjestelmää. Jotta digitaalista turvallisuutta voidaan johtaa oikein, tulee yrityksen ymmärtää tietoturvan mittaaminen organisaatioiden eri tasoilla. Mittaamista ja tietoturvallisuuden tasoja on tarkasteltu työn kappeleissa 2.4 ja 2.5.

Luvussa kolme käsitellään digitaalisen turvallisuuden prosesseja ja syvennytään tarkemmin käsittelemään termistöä sekä eri osa-alueiden sidonnaisuuksia digitaaliseen turvallisuuteen. Merkittävin digitaalisen turvallisuuden hallintaprosessi on riskienarviointi. Kappaleessa 3.4 keskitytään riskien hallintaan vertailemalla digitaalisen turvallisuuden riskimatriisia Yaran omaan työturvallisuuden riskienarviointimatriisiin. Riskejä ei koskaan voida kokonaan poistaa, vaan toiminnassa tulee tunnistaa mahdolliset vaaratekijät ja hallita ne siten, että toimintaan liittyvä riski on hyväksyttävän alhaisella tasolla.

Työn luvussa neljä käsitellään ja esitellään Yaran toimintamalleja henkilöstölle, liittyen digitaalisen turvallisuuden hallintaan. Ohjeet ja käytännöt ovat saatavilla yrityksessä hyvin, mutta ne on hajautettu useamman organisaation alle ja tämä luku toimii tiivistelmänä henkilöstölle liittyen digitaalisen turvallisuuden hallinnan keinoihin. Luvussa esitellään myös Yaralla toteutettuja, simuloituja phishing kalastelukampanjoita ja niiden tuloksia.

Opinnäytetyön luku viisi peilaa yrityksen digitaalisen turvallisuuden nykytilaa DNV:n itsearviointityökaluun ja tämän avulla on etsitty parannuskeinoja, jotka tässä luvussa esitetään opinnäytetyön johtopäätöksinä. Yhteenvetona löydetyistä parannuskohteista esille nousevat: henkilökunnan koulutuksen lisääminen, kolmansien osapuolten huomioiminen digitaalisen turvallisuuden koulutuksissa sekä palautumissuunnitelmien syventäminen ja toimintamallin harjoittelu käytännössä. Luvussa viisi on myös omaa pohdintaani liittyen digitaalisen turvallisuuteen, tämän opinnäytetyön toteutukseen ja tulevaisuuden näkymiin digitaalisen turvallisuuden tiellä.

LÄHTEET

BYRES, E. (2013). The Industrial Cybersecurity Problem. *ISA WHITE PAPER*.

CYBER DEGREES, b. (2019, December 11). *Cyber Security Jobs*. Retrieved from https://www.cyberdegrees.org/jobs/

D'antonio, G. (2019, 8 5). *IN sights, articles*. [viitattu 2020-3-22] Saatavissa: https://www.ie.edu/insights/articles/the-future-is-upon-us/

DNV. (2020). *ISO 27001 tietoturvajärjestelmä*. [viitattu 2020-1-20] Saatavissa: https://www.dnvgl.fi/services/iso-27001-tietoturvajarjestelma-3327

JÄRVINEN, P. (2018). Esitysmateriaali.

JÄRVINEN, P. (2018). *Kyberuhkia ja somesotaa.* Docendo.

KPMG. (2016). Tietoturvan hallinta.

KPMG. (2019). Esitysmateriaali, Pauli Wihuri.

PIRHONEN, J. (2018, January 9). Digitaalisen turvallisuuden hallinta.

TIETO. (2019). Riskienhallintaprosessi.

TIETOSUOJA. (2019, December). *GDPR*. [viitattu 2020-1-15] Saatavissa: https://tietosuoja.fi/dgpr

TIETOSUOJA. (2019). *Tunne oikeutesi*. [viitattu 2020-1-15] Saatavissa: https://tietosuoja.fi/tunne-oikeutesi

TRAFICOM. *Kyberturvallisuuskeskus - Kybersaa.* [viitattu 2020-2-24] Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4_tammikuu_2020.pdf

TRAFICOM. (2020). *Kyberturvallisuuskeskus - Varoitukset*. [vitattu 2019-12-11] Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/varoitukset

VALTIONVARAINMINISTERIÖ. *Vahtiohje*. [vitattu 2019-12-11] Saatavissa: https://www.vahtiohje.fi/web/guest/home

VIITAILA, M. (2019). Kyberturvallisuus älykkään reunan maailmassa. *Automaatioväylä*, 12-13.

YARA. (2019). 50 vuotta juhlamateriaali, Yara Suomi Oy. Siilinjärvi.

YARA. (2019). GDPR ohje, International ASA. Oslo.

YARA. (2019). International ASA. Oslo.

YARA. (2019). Physical Security, International ASA. Oslo.

YARA. (2019). Yara Information Handling, International ASA. Oslo.

YARA. (2019a). Yara Security Management, International ASA. Oslo.

YARA. (2019b). Yara End User Policy, International ASA. Oslo.

YARA. (2020). Esittelymateriaali, Yara Suomi Oy. Siilinjärvi. [Viitattu 2020-2-23]. Saatavissa: https://www.yara.fi/tietoa-yarasta/

DNV·GL

INFORMATION SECURITY MANAGEMENT SYSTEM

Self Assessment

Have you implemented the 10 essential information security controls?

No matter what the size of your business or scope of operation, managing your information security risks is vital. ISMS (Information Security Management System) certification provides the confidence that any risk to information held by the organization is systematically managed.

There are 10 essential controls that are fundamental building blocks for information security management systems. This sample question set allows you to self assess your information security controls against those 10 essentials.

 DNV GL AS, NO-1322 Høvik, Norway, Tel: +47 67 57 99 00, www.dnvgl.com

1. Information Security Policy

1.1.1 We have written security policy document(s) approved by top management.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

1.1.2 The security policies are available and communicated to all staff.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

1.1.3 The security policies are updated periodically.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

1.1.4 We conduct regular reviews to confirm compliance with security policies and standards e.g. technical compliance checks, system audits.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

2. Assessment of security risks

2.1.1 We have identified an appropriate method for security risk assessment.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

2.1.2 We have systematically considered the business harm and the likelihood of security breaches.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

2.1.3 We have evaluated the security risks against criteria for acceptance and are taking appropriate actions for risks outside the criteria.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

3. Allocation of security responsibilities

3.1.1 We have defined the overall responsibilities for protection of information and IT assets.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

3.1.2 Each information system is the responsibility of a defined system owner.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

3.1.3 Responsibilities for the implementation of security processes is also clearly defined.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

4. Training awareness and education

4.1.1 Users receive appropriate training in security policies and procedures.

- ☐ Fully
- ☒ Largely
- ☐ Partly
- ☐ Not done

4.1.2 There is an active security awareness programme in operation.

- ☒ Fully
- ☐ Largely
- ☐ Partly
- ☐ Not done

4.1.3 Users receive training in the correct use of information systems.

- ☐ Fully
- ☒ Largely
- ☐ Partly
- ☐ Not done

4.1.4 This training also extends to third party users.

- ☐ Fully
- ☐ Largely
- ☐ Partly
- ☒ Not done

4.1.5 Staff and 3rd parties with access to our information systems sign non-disclosure agreements.

- ☐ Fully
- ☐ Largely
- ☒ Partly
- ☐ Not done

5. Security incident management

5.1.1 There is a formal reporting procedure for security incidents.

- ☒ Fully
- ☐ Largely
- ☐ Partly
- ☐ Not done

5.1.2 All staff and third parties are made aware of the incident reporting procedure.

- ☐ Fully
- ☐ Largely
- ☒ Partly
- ☐ Not done

5.1.3 Security incidents are reported quickly through management channels.

- ☐ Fully
- ☐ Largely
- ☒ Partly
- ☐ Not done

5.1.4 There is a formal disciplinary process for security breaches.

- ☐ Fully
- ☐ Largely
- ☒ Partly
- ☐ Not done

6. Protection from cyberspace attack

6.1.1 We prohibit the use of unauthorised software.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

6.1.2 We have deployed programs and measures to protect against malicious software e.g. viruses, trojan horses, malware.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

6.1.3 We have deployed measures to protect against external 'hacker' attacks e.g. IDS, Firewalls, DMZ.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

6.1.4 There are regular reviews of software and data on critical systems to detect any unauthorised programs or data.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

7. Business continuity planning

7.1.1 We develop and maintain business continuity plans according to a managed process.

- [ ] Fully
- [ ] Largely
- [x] Partly
- [ ] Not done

7.1.2 The risks from events that could interrupt business are identifed and evaluated e.g. fire, flood, major accident; pandemic, utility failure.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

7.1.3 Continuity plans enable us to maintain operations following failure or damage to vital services and facilities.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

7.1.4 Continuity plans are tested and updated regularly.

- [ ] Fully
- [ ] Largely
- [x] Partly
- [ ] Not done

8. Misuse of proprietary software

8.1.1 We require staff to comply with software license conditions.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

8.1.2 We maintain up-to-date registers of software licenses.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

8.1.3 We conduct regular audits of software use.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

9. Safeguarding enterprise data

9.1.1 Inventories of key enterprise data sources are maintained.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

9.1.2 We have guidelines for retention, storing and disposal of data and records.

- [ ] Fully
- [ ] Largely
- [x] Partly
- [ ] Not done

9.1.3 We have implemented measures to protect stored enterprise data from loss or corruption.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done

10. Personal data protection

10.1.1 We have a management structure and controls to comply with data protection legislation.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

10.1.2 Data owners have responsibility to identify any personal information that is stored or proposed for storage.

- [x] Fully
- [ ] Largely
- [ ] Partly
- [ ] Not done

10.1.3 We report the personal data being stored and the purposes for its use in accordance with applicable legislation e.g. Data Protection Act 1998.

- [ ] Fully
- [x] Largely
- [ ] Partly
- [ ] Not done